IMPACTS OF MALICIOUS CYBER ACTIVITIES

by
Alex Leon

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Global Security Studies

Baltimore, Maryland
August 2015

Abstract

In past decades security dilemmas focused on state on state activities where the tools of power were only obtainable with the resources a state can bring to bear. In moving into a new era where the cyber domain offers state and non-state actors the ability to wield low-cost capabilities for high-effect actions, understanding the implications of these threats to national security is paramount.

This thesis ponders if proposed cyber governance models are effective in assessing risk, preventing, and responding to malicious cyber activities. Current governance processes for preventing and responding to malicious cyber activities are immature and inadequate to manage the requirements of an ever-expanding cyber domain. This thesis explores why current approaches to implementing security through policy and standards of practice have been unsuccessful and concludes that evidence found though analyzing multiple case studies shows a lack of coherent risk assessment, inadequate prevention and inconsistent responses to malicious cyber activities.

The first chapter explores whether governance approaches designed to prevent and deter malicious cyber activities are effective, hypothesizing that current governance processes cannot deter or prevent malicious cyber activities. Through the analysis of the 2013 Target and the 2014 USIS computer network exploitation in relation to three governance approaches

explored in the literature review, analysis revealed none provided adequate cyber incident prevention.

The second chapter explores governance approaches to respond to malicious cyber activities are effective, hypothesizing that current response options are not effective. Through the analysis of the 2014 Sony and 2014 JP Morgan Chase malicious cyber incidents, response approaches reviewed were inadequate in part because of legal authority but poor risk assessment also emerged as a driving factor.

The final chapter explores whether a state actor, in this case China is a risk to critical infrastructure. The chapter theorizes that state actors such as China possess the capability to conduct crippling cyberattacks in U.S. critical infrastructure. Using the 2003 northeast blackout as an analog the chapter concludes that though cyberattacks on U.S. critical infrastructure are possible, wide scale full spectrum cyber warfare is unlikely; however the threat that state actors pose to the U.S. infrastructure is real, and requires further attention.

Thesis Reviewers:
James Norton
Michael Warner

Table of Contents

List of Tables

Table of Figures

Thesis Introduction

In past decades security dilemmas focused on state on state activities where the tools of power were only obtainable with the resources a state can bring to bear. As we move into a new era where the cyber domain offers state and non-state actors the ability to wield low-cost high-effect capabilities, understanding the implications of this new domain to security is paramount. To develop policies, doctrine and standards of practice the implications of malicious activities with regard to security must be determined. This thesis explores why current approaches to implement security through policy approaches have been unsuccessful. Indications imply that the reason current approaches have failed is lack of attention to the fundamental problem of providing security through policies that have little or no deterrent effect.

Throughout history, humanity has found new and interesting ways to leverage virtually any medium to conduct commerce and warfare. Naturally, the domains of warfare—land, sea, undersea, air, and space—were used in the order they were discovered and defined as technology evolved. Commerce has also leveraged these same channels for the conduct of private and state business. As these domains evolved and their use proliferated, agreements emerged to codify conduct, in both peace and crisis, within these domains. Arranged in a myriad of treaties, and bilateral and multilateral agreements, these accords of peace, laws of war and treaties of trade provide standards for

how states conduct themselves in the global commons. Through these pacts, states maintain stability by reducing misunderstandings during times of harmony and crisis. Some pacts are designed to prevent crises. For example, the Chemical Weapons Convention, an international treaty ratified by most countries, bans the production, acquisition, and use of chemical weapons, thus reducing the risk of war using chemical weapons.[1] Other standards provide stable infrastructure support, such as the international communications standards managed by the International Institute of Communications.[2]

The cyber domain is a global asset in many ways similar to the space domain. However, because much of it manifests virtually the cyber domain is distinct from the other domains. It is the first domain that is entirely man made and the only domain that exists in all other domains concurrently. Cyber is the only domain where actions and reactions can traverse the globe almost instantaneously with the click of a button. The cyber domain is unique because it equalizes humanity, providing equal power status between nation states and even individuals. The cyber domain can also be leveraged for malicious effects across normal sovereign boundaries.[3] Unlike the physical

---

[1] Organisation for the prohibition of chemical weapons. "Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction." *Organisation for the prohibition of chemical weapons.* July 29, 2005. https://www.opcw.org/index.php?eID=dam_frontend_push&docID=6357 (accessed April 7, 2015).

[2] International Institute of Communications. *International Institute of Communications.* April 6, 2015. http://www.iicom.org/ (accessed April 6, 2015).

[3] Defense Science Board. "Resilient Military Systems and the Advanced Cyber Threat." *Defense Science Board.* January 2013. http://www.acq.osd.mil (accessed 09 15, 2013): 46.
Mandiant. "APT1: Exposing One of China's Cyber Espionage Units." *Mandiant Intelligence Center Report.* February 18, 2013. http://intelreport.mandiant.com (accessed 09 25, 2013): 2-3.

domains of air, sea, land and space, the cyber domain is unique in that activities within the domain may not be recognized as malicious, and, even if they are recognized as such, there may be no plausible way to determine the initiating party.[4] Lastly, the cyber domain is the only one in which the civilian, government and military portions are deeply intertwined.[5] In the cyber domain the lines connecting the sectors blur, occasionally fading completely, making it extremely difficult to distinguish between civilian, government and military actions.

Chapter 1: Policy Response Approaches

In the first chapter of this thesis, the current laws, policies, regulations, treaties, and other governing documents designed to implement standards on the Internet are examined to assess the various governance approaches offered. The intent of the chapter is to determine the intended effects and overall effectiveness of these policy approaches with regard to creating stability, insuring security, and avoiding misunderstandings in any response approaches. The chapter hypothesizes that governance approaches to date have failed to provide adequate cybersecurity. Further, there may not be cyber policy approach that provides security without fundamental changes to the base infrastructure of the Internet.

---

[4] Ashford, Warwick. "Problems in attributing cyberattacks could foil US sanctions against hackers." *Computer Weekly*, April 14, 2015: 4.
Schmidt, Howard, interview by Cameron and Mustafa Safdar Parsons. *Defending Cyberspace: The View from Washington* (April 11, 2011).
[5] Defense Science Board. (January 2013): 5.

The approaches were grouped into three categories for ease of assessment: polycentric governance, state centric governance, and active defense. The identified governance approaches are examined through the analysis of two cyber incident case studies.

The first case presented is a private sector centered cyber incident: the 2013 computer network exploitation on Target stores. This malicious cyber incident provided an analog to evaluate the various methods of governance with what happened. The second case study in this chapter was a comprehensive look at the U.S. Investigations Services computer network exploitation of 2014. This case was chosen to represent an example of a malicious cyber incident where the government, through multiple legal vectors, has more authority to intervene than in the Target case.

The chapter shows that perhaps the best model for governance is a combination of polycentric governance, state centric governance, and active defense. The ultimate solution may need to be a fundamental change to the base structure of the Internet that provides the security necessary in a world where the technologies driving forward innovation and growth is the same one that may be the vehicle to cause the next world war.

Chapter 2: Economic Impacts of Malicious Cyber Incident Response

The second chapter in this series examines the threat to the United States economy through malicious cyber activities and the possible responses.

Current response options are tested using two case studies to determine if the options available provide adequate solutions. The chapter hypothesizes that the response options available (e.g. active defense and state centric) do not result in timely response to malicious cyber activities. Furthermore, in order to respond to malicious cyber activities fundamental changes to response approaches must be made.

The chapter reviews two recent cyber incidents: 2014 computer network exploitation at JP Morgan Chase and a 2014 cyberattack at Sony. These cases were chosen to compare and contrast the government and industry response to each incident. The robust government reaction to the Sony cyberattack in contrast to the JP Morgan Chase computer network exploitation incident is examined in this chapter, since the relative risk to national security in the JP Morgan Chase case is higher than that of the Sony attack.[6]

The chapter concludes that despite contrasting views regarding the attribution of the Sony attacks and the subsequent government response the U.S. government does not have a sufficient method to assess cyber incident risk factors.[7] The lack of timely weighted risk assessment is a factor that leaves the government and industry unable to respond to malicious cyber incidents in a more effective way. Future solutions will have to address the

[6] Department of Homeland Security. (November 2013).
[7] Berghel, H. "Cyber Chutzpah: The Sony Hack and the Celebration of Hyperbole." *Computer* 48, no. 2 (February 2015): 77-80.

current legal issues that hamper government and private industry collaboration.[8]

Chapter 3: Threat to Critical Infrastructure

The final chapter of this thesis explores the risk to United States critical infrastructure by cyber actors using Computer Network Attack (CNA) techniques on networked computer command and control and supporting systems.[9] The chapter assesses malicious cyber actor capabilities and intent, examining the vulnerability of the select targets, mitigations to those vulnerabilities currently in place, and potential consequences of an attack to the selected targets. Potential mitigation techniques for the assessed vulnerabilities are evaluated for effectiveness and practicality of implementation.

The chapter approaches the assessment by defining the threat through a standard model. The focus of the chapter is on the capabilities and intent of malicious actors using a Chinese state actor model. The case studies looked at the 2003 blackout in northeastern United States and Canada. The various cyber incident vectors were compared to the event to determine the feasibility of a similar incident occurring from state sponsored malicious cyber activities.

---

[8] Fischer, Eric A., Edward C. Liu, John W. Rollins and Catherine A. Theohary. *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress.* Report, Congressional Research Service, Washington, D.C.: International Security & Counter Terrorism Reference Center, December.
Givens, Austen D., and Nathan E. Busch. "Integrating Federal Approaches to Post-Cyberattack Mitigation." *Journal of Homeland Security & Emergency Management* (International Security & Counter Terrorism Reference Center) 10, no. 1 (April 2013): 1-28.

[9] Department of Homeland Security. *dhs.gov*. November 15, 2013. http://www.dhs.gov/what-critical-infrastructure (accessed 11 15, 2013).

The chapter concludes that though there is a possibility that state sponsored cyber teams could disable, disrupt and even destroy U.S. critical infrastructure, the evidence suggests that wide scale full spectrum cyber warfare is not currently feasible. However, in many cases even minor attacks to critical infrastructure are dangerous due to unpredictable ripple effects.

Chapter 1: Policy Response Approaches

Introduction

This chapter examines the current laws, policies, regulations, treaties, and other governing documents that attempt to implement standards on the Internet. The governance approaches identified in the literature review are used to analyze two cyber incident case studies. The analysis is used to determine the intended effects and overall effectiveness of these policy approaches with regard to creating stability, insuring security, and avoiding misunderstandings. Next, the chapter presents a literature review, and then explores each case, concluding that there is no evidence that any of the examined policy processes would deter or prevent malicious cyber incidents from a determined malicious actor.

Much of the current discussion about U.S. cyber policy focuses on the establishment of fair use agreements, cyber defense, and cyber normality and avoids more difficult policy discussions that must define a cyberattack and what types of attacks are an act of war.[10] While this chapter does not explore the topic, research is needed in the area of defining reasonable justification for the conduct of cyber, conventional, or nuclear retaliation following a cyber-enabled attack. What this chapter seeks to explore are the conceptual solutions for cybersecurity through policy regulation, standards of conduct,

[10] Coldebella, Gus P., and Brian M. White. "Foundational Questions Regarding the Federal Role in Cybersecurity." *Journal Of National Security Law & Policy* (International Security & Counter Terrorism Reference Center) 4, no. 1 (January 2010): 242.
Contreras, Jorge L., Laura Denardis, and Melanie Teplinsky. "Mapping Today's Cybersecurity Landscape." *American University Law Review* (Index to Legal Periodicals & Books) 62, no. 5 (June 2013): 1121.

treaties, rules, laws and any other concepts being put forth. Some of these concepts have been captured officially (e.g. presidential directives), while others have only been theorized.

Unlike physical domains, cyber is unique because malicious actions are often mistaken as non-malicious, or, not detected at all. The reality that even recognized malicious activities might not be feasibly tracked back to the initiating party further complicates response options.[11] In the cyber domain, the enemy is transparent and often actions that resemble attacks can resemble defense, and vice-versa. Further, actions in the cyber domain often do not have a correlating effect in the physical world. This has implications for both the attacker and the defender. The attacker often cannot assess damage and defenders cannot assess if the activity was an attack.[12] These factors make the cyber domain one of constant ambiguity, resulting in decreased ability to avoid misunderstandings.

Establishing policies for the cyber domain is crucial to avoid miscalculations between nation states. The unique aspects of the cyber domain and the overall infancy of the globally connected Internet make the development of acceptable laws and policies governing the fair use of the cyber domain complex. Without the establishment of policies, fair use, and

[11] Ashford, Warwick. (April 14, 2015): 4.
[12] Greenberg, Andy. McAfee Explains The Dubious Math Behind Its 'Unscientific' $1 Trillion Data Loss Claim. August 03, 2012. http://www.forbes.com (accessed 10 21, 2013).

conduct agreements, malicious activities could spiral out of control causing cyber, conventional, or even nuclear war.

What is the Cyber Domain?

What can be asserted with minimal debate is that cybersecurity and the cyber domains are amorphous concepts. To define cybersecurity it is necessary to first develop a sense of what the cyber domain is and from what, or in many cases, from whom it is being secured.[13] Multiple actors seek to exploit cybersecurity vulnerabilities to conduct nefarious activities for a myriad of reasons. There are several suggested ways to define the cyber domain. Cyber domain has been described as a new war fighting domain, a global commodity, and a communications system. Additionally, some see the cyber domain as a combination of all three.[14]

A fitting way to understand the cyber domain is to imagine a non-biological entity that is evolving on a continuous basis. The cyber domain was never designed to be secure; it was designed to communicate data between trusted actors. The lack of integrated security combined with contiguous evolution suggests that any attempt to add security is extremely difficult. Regardless of how the cyber domain is defined, the underlying insecurity of the system drives a serious debate with regard to cybersecurity and the

---

[13] Defense Science Board. (January 2013): 21.
[14] Hunker, Jeffrey. "U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away." *Journal of National Security Law & Policy* (International Security & Counter Terrorism Reference Center) 4, no. 1 (2010): 197-216.
Malone, Eloise F., and Michael Malone. "The "wicked problem" of Cybersecurity policy: analysis of United States and Canadian policy response." *Canadian Foreign Policy Journal* 19, no. 2 (August 2013): 158-177.

policies, laws and regulatory actions that may be required to maintain the integrity of the system.[15]

Perhaps the most vexing issue for lawmakers to overcome in mandating cybersecurity is the ownership of the cyber domain. One reason this adds complexity is an assessment that 85% of the U.S. controlled critical cyber infrastructure is privately owned.[16] The portions that are federally owned, in many cases, also transmit data over privately owned equipment or infrastructure such as underground fiber optics, switching stations, and electrical power generation.[17] The private nature of this infrastructure makes regulation very difficult without violating constitutional protections. There are other competing factors in the development of cybersecurity solutions such as the separate, and in many cases competing, security implementation actors: the national security and intelligence community, the military, law enforcement, legal and regulatory experts, companies, and cyber privacy advocates.[18]

The complexity of the cyber domain and the breadth of conceivable threats that can be projected through the cyber domain require careful study

---

[15] United States Senate, One Hundred Sixth Congress. Internet Security: Hearing before the Subcommittee On Communications of the Committee On Commerce, Science, and Transportation. Second Session, Washington, D.C.: G.P.O., 2000.
[16] Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. "Cybersecurity and US Legislative Efforts to address Cybercrime." *Journal Of Homeland Security & Emergency Management* (International Security & Counter Terrorism Reference Center) 10, no. 1 (April 2013): 1-27.
[17] Defense Science Board. (January 2013): 76.
[18] Malone, Eloise F., and Michael Malone. (August 2013): 171.

and consideration to determine the most equitable method of security while maintaining freedoms protected under the constitution.[19]

Literature Review

This literature review helps identify ideas that resonate in the assessed literature, including the ideas that show commonality and the unique thoughts regarding cybersecurity policy. The debate over cybersecurity, and, importantly, by whom and how the cyber domain should be secured, has multiple complexities. Two of these complexities include who should secure the Internet and how it should be secured. Opinions on Internet security management policies often follow closely with who manages them, though they do not always synchronize.

Polycentric Governance Approach

There are multiple viewpoints regarding who should regulate the Internet. One of the most discussed ideas is polycentric governance.[20] The concept is rooted in the heterogeneous nature of the cyber domain where no one individual, state, or international body has full ownership or management over the whole domain.[21] This concept is most consistent with the current ownership model of the cyber domain. Establishing behavior

[19] McAfee. "A Good Decade for Cybercrime." *www.mcafee.com*. December 29, 2010. http://www.mcafee.com (accessed October 21, 2013): 4.
[20] Brechbuhl, Hans, et al. "Protecting Critical Information Infrastructure: Developing Cybersecurity Policy." *Information Technology for Development* (Business Source Complete) 16, no. 1 (January 2010): 83-91.
Contreras, Jorge L., Laura Denardis, and Melanie Teplinsky. (June 2013): 1121.
Shackelford, Scott J, and Amanda N Craig. "Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity." *Stanford Journal Of International Law* (Academic Search Complete) 50, no. 1 (2014): 119-184.
Singh, J. P. "Multilateral Approaches to Deliberating Internet Governance." *Policy & Internet* 1 (2009): 91-111.
[21] Defense Science Board. (January 2013): 1.

norms for the cyber domain is a concept that manifests individually but is also present in the polycentric governance framework.[22] The concept is rooted in the idea that through the development of cyber norms Internet users will maintain security through best practices. Other ideas in the literature revolve around protectionist themes such as centralizing government cybersecurity, legislating 'voluntary' standards, and moving to an active defense posture.[23]

While the basic idea of polycentric governance is common, the concept manifests in several ways throughout the literature. In several studies, the authors only discuss the idea of polycentricism within the state itself.[24] This view focuses on the interaction between the state and commercial or private actors. The model presents a view where the cyber domain is regulated through a collaborative effort with representatives from each of the interested parties to determine best practices and implementation. In this concept, the model accepts the amorphous nature of the Internet and attempts to overcome the complexity by accepting it and dividing the responsibility for security among a wide range of actors.

---

[22] Brechbuhl, Hans, et al. (January 2010): 87.
Hunker, Jeffrey. (2010): 197-216.
[23] Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. (April 2013): 1-27.
Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. "Leaving Deterrence Behind: War-Fighting and National Cybersecurity." *Journal Of Homeland Security & Emergency Management* (International Security & Counter Terrorism Reference Center) 7, no. 1 (January 2010): 1-24.
Hunker, Jeffrey. (2010): 197-216.
Newmeyer, Kevin P. "Who Should Lead U.S. Cybersecurity Efforts?" *PRISM Security Studies Journal* (International Security & Counter Terrorism Reference Center) 3, no. 2 (March 2012): 115-126.
[24] Broggi, Jeremy J. "Building on Executive Order 13,636 to Encourage Information Sharing for Cybersecurity Purposes." *Harvard Journal Of Law & Public Policy* (Business Source Complete) 37, no. 2 (2014): 653-676.

In other examples of polycentric approaches, the multipronged governance structure accounts for the global nature of the cyber domain by suggesting that states, businesses, individuals, and international bodies must work together to maintain the integrity of the system.[25] This approach suggests that security must also be accomplished through bilateral and multilateral security and conduct agreements. The idea of implementing a governance structure to account for the interconnectedness of the cyber domain is one of necessity in some cases and practicality in others. The necessity argument often falls into several categories that revolve around enforcing laws.[26] These are usually criminal laws but states and individuals are concerned with the enforcement of trading rules and procedures as well as international contract laws, copyrights, and patents.

The strengths of polycentric approaches are in the acceptance of the plurality of ownership, the lack of defined borders and boundaries, and the complexity of the interconnectedness of the cyber domain. The authors who explored governance through the lens of ownership plurality gave suggestions that encompassed more than just a specific nation state's perceived portion of the Internet.[27] In turn, this allowed the authors to consider solutions that, if enacted, could be used for more than one stakeholder.

---

[25] Brechbuhl, Hans, et al. (January 2010): 83-91.
DeNardis, L. "E-Governance Policies for Interoperability and Open Standards." *Policy & Internet* 2 (2010): 129–164.
[26] Newmeyer, Kevin P. (March 2012): 115-126
[27] Contreras, Jorge L., Laura Denardis, and Melanie Teplinsky. (June 2013): 1113-1130.

Multipronged or polycentric governance arguments lack discussion regarding the difficulty of resolving complex issues between the relevant states, the government institutions, corporations, and private citizens. Some even suggest that the traditional regulatory and legal procedures will not work at all.[28] Some of the studies attempt to present models for new global Internet governance institutions or at least recognize that without some new form of regulating body the idea of polycentric or multipronged governance is not a viable solution.[29]

State Centric Governance Approach

A separate common theme presents a model of state centric regulation and control over the cyber domain.[30] These ideas appear to revolve around the basic tenant of getting one's own house in order first.[31] Most of these solutions seek government action through legislation that involves centralizing control over government cybersecurity, improving cyber governance procedures, promoting cyber norms and encouraging private sector participation with a government lead.[32] For more than fifteen years,

---

[28] Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. (January 2010): 1-24.
Malone, Eloise F., and Michael Malone. (August 2013): 158-177.
[29] Contreras, Jorge L., Laura Denardis, and Melanie Teplinsky. (June 2013): 1113-1130
[30] Broggi, Jeremy J. (2014): 653-676.
Hunker, Jeffrey. (2010): 197-216.
Newmeyer, Kevin P. (March 2012): 115-126.
U.S. Govt. Accountability Office. Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use. Report to Congressional Committees, Washington, D.C.: U.S. Govt. Accountability Office, 2011.
[31] Coldebella, Gus P., and Brian M. White. (January 2010): 233-245.
[32] Broggi, Jeremy J. (2014): 653-676.
Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. (April 2013): 1-27.
Hunker, Jeffrey. (2010): 197-216.
Newmeyer, Kevin P. (March 2012): 115-126.
Shackelford, Scott J, and Amanda N Craig. (2014): 119-184.

the United States government has recognized the need to manage cybersecurity. Yet as multiple United States Government Accountability Office (GAO) reports suggest, there has been minimal progress.[33]

Studies of state centric regulation tend to focus on activities that concentrate on regulating state controlled networks.[34] This approach suggests that to manage the security of critical infrastructure the government must first secure its own networks. While there have been multiple proposals for making this achievable, to date, the concept is still very difficult to implement.[35] The implementation of standardized security practices by governments can be difficult, however, because numerous stakeholders want to maintain control over their individual networks.[36] A centralized government management structure for cybersecurity implies some loss of control by the individual stakeholders such as the State Department or Defense Department. Further, governmental structure and laws regulating

---

[33] U.S. Government Accountability Office. *Internet Infrastructure: DHS Faces Challenges In Developing a Joint Public/private Recovery Plan.* Report to Congressional Requesters, Washington, D.C.: U.S. Government Accountability Office, 2006.
U.S. Govt. Accountability Office. Critical Infrastructure Protection: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology. Report to the Congressional Requesters, Washington, D.C.: U.S. Govt. Accountability Office, 2014.
U.S. Govt. Accountability Office. Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. Report to Congressional Requestors, Washington, D.C.: U.S. Govt. Accountability Office, 2013.
U.S. Govt. Accountability Office. Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative. Report to Congressional Requesters, Washinton, D.C.: U.S. Govt. Accountability Office, 2010.
U.S. Govt. Accountability Office. Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed. Report to Congressional Requesters, Washington, D.C.: U.S. Govt. Accountability Office, 2010.
U.S. Govt. Accountability Office. *Cyberspace: United States Faces Challenges In Addressing Global Cybersecurity and Governance* . Report to Congressional Requesters, Washington, D.C.: U.S. Govt. Accountability Office, 2010.
[34] Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. (January 2010): 1-24.
Hunker, Jeffrey. (2010): 197-216. Newmeyer, Kevin P. (March 2012): 115-126.
[35] DeNardis, L. (2010): 129–164.
Klimburg, Alexander. National Cybersecurity Framework Manual. NATO CCD COE Publications, 2012.
[36] U.S. Govt. Accountability Office. "Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative". (2010).

access to information can also make it difficult to centrally manage security. For example, there are many laws that pertain to sharing of domestic information between intelligence agencies but the relative effectiveness of the laws comes into question upon implementation.[37]

Additionally, studies suggest the government may be attempting to move beyond managing its own networks and instead expand into the private sector through various legal and cooperative frameworks. Recently the Federal Communications Commission voted on the enactment of a set of rules that will attempt to govern some activities on the Internet.[38] Known as the Net Neutrality or Open Internet rules, they seek to set commercial practices in place to manage Internet traffic.[39] One of the other activities slowly being adapted from a voluntary action to a requirement is the disclosure of cybersecurity risks to the Securities and Exchange Commission.[40]

Some of the studies analyzed the relationship between the government and the authorities under which it might regulate the Internet. Opderbeck argued that legal authority to regulate the Internet was mired in constitutional protections and thus difficult to navigate with laws and regulations.[41] Regardless, he argued that the Executive branch should have

---

[37] U.S. Govt. Accountability Office. (2011).
[38] Albanesius, Chloe. "Why 2015 May Be the Year We Solve Net Neutrality." PC Magazine, February 01, 2015: 12.
[39] Ibid: 12.
[40] Grant, Gerry H., and C. Terry Grant. "SEC Cybersecurity Disclosure Guidance is Quickly Becoming a Requirement." *CPA Journal* (Business Source Complete) 84, no. 5 (June 2014): 69-71.
[41] Opderbeck, David W. "Cybersecurity and Executive Power." *Washington University Law Review* (Index to Legal Periodicals & Books) 89, no. 4 (May 2012): 795-845.

emergency authority to take unilateral actions.[42] This argument is contrasted by assessments in other writings that suggest the authority to take emergency executive action requires capabilities that do not exist. For example, Opderbeck explored the possibility of using the Communications Act of 1934 in allowing for an Internet kill switch.[43] The assumption that in an emergency the President or an act of Congress could authorize the cutoff of Internet services may be politically and even legally viable in some instances; however, literature indicates that the difficulty resides in executing the action.[44]

The writings in the state centric governance group are strong in the assessment of current shortfalls in the abilities of the United States to manage its own government networks.[45] The writings also take into account the difficulties in regulating the infrastructure that the vast majority of the Internet traffic traverses. This recognition allows the authors to parse this complex issue into seemingly manageable portions. Using that process they excel at describing the probable ways the government could take action to

---

[42] Opderbeck, David W. (2012): 844.
[43] Opderbeck, David W. "Does the Communications Act of 1934 Contain a Hidden Internet Kill Switch?." *Journal Federal communications law journal* 65, no. 1 (January 2013): 1-46.
[44] Opderbeck, David W. (2012): 807
[45] Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. (April 2013): 1-27.
Greenwald, Eric A. "History Repeats Itself: The 60-Day Cyberspace Policy Review in Context." *Journal of National Security Law & Policy* (International Security & Counter Terrorism Reference Center) 4, no. 1 (January 2010): 41-62.
Heilbrun, Mark R., and Isaac Brown. "Cybersecurity Policy and Legislation in the 112th Congress." *Intellectual Property & Technology Law Journal* (Business Source Complete) 23, no. 12 (December 2011): 14-20.

shore up defenses and to implement proactive steps to thwart future threats.[46]

The shortfalls in these writings focus on centralized solutions for an amorphous problem. The emphasis on centralized solutions ignores many of the issues the polycentric governance authors suggest. These writings in many cases either dismiss or ignore the global nature of the cyber domain and the regulatory issues that encompasses.

Active Defense Approach

The literature reviewed contained several unique thoughts, however the most compelling thought that appeared in a couple different forms revolved around the idea of the United States setting cyber deterrence aside and adopting a full war-fighting posture.[47] This idea was unique in its presentation by Harknett but other authors attempted to provide language in their assessments that leaned in the direction of a war-fighting posture through the suggestion of active defense, moving away from passivity and defining the justification for military action in the cyber domain.[48]

While an interesting thought, the weakness in this argument remains: there is no current precedent for the conduct of war in the cyber domain.

---

[46] Contreras, Jorge L., Laura DeNardis, and Melanie Teplinsky. (June 2013): 1113-1130.
Flowers, Angelyn, and Sherali Zeadally. "US Policy on Active Cyber Defense." *Journal Of Homeland Security & Emergency Management* (International Security & Counter Terrorism Reference Center) 11, no. 2 (June 2014).
Hunker, Jeffrey. (2010): 197-216.

[47] Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. (January 2010): 1-24.

[48] Flowers, Angelyn, and Sherali Zeadally. (June 2014).
Hunker, Jeffrey. (2010): 197-216.
Schwitz, John G. "Risk-Based Cybersecurity Policy." *American Intelligence Journal* (International Security & Counter Terrorism Reference Center) 29, no. 1 (March 2011): 115-125.

While there are words on paper that define cyber defense, cyber strategy and cyber policy, the doctrine, training, methodologies, tactics, techniques and procedures are far from perfect.[49] The authors suggest one solution is active defense: activities conducted to retaliate against a malicious actor or take other proactive measures rather than simply blocking them. The writings suggest that active defense actions may not be in the best interest of those executing them. Active defense methodologies could escalate a cyberattack if misunderstood by the attacker as an offensive action.[50]

The strength in this argument is the acknowledgement that governments need to categorize malicious activities and respond to them in a manner appropriate for the risk and damage the activities could cause to state and private property. This argument also looks only at the state and its needs, which in many cases is much easier to control and manage.[51] These writings also lack attention to the implications of strengthening the defenses the government-controlled side of the cyber domain that rely on the privately controlled portions to function.[52] Lastly, though the authors do consider that active defense may escalate into conventional or even nuclear war they do not provide suggested solutions to avoid these possible risks.

---

[49] Department of Defense. "Defense.gov." *Department of Defense Strategy for Operating in Cyberspace.* July 2011. http://www.defense.gov (accessed September 25, 2013).
Department of Defense. "Department of Defense Cyberspace Policy Report." *www.defense.gov.* November 2011. www.defense.gov (accessed September 15, 2013).
[50] Defense Science Board. (January 2013).
Flowers, Angelyn, and Sherali Zeadally. (June 2014).
[51] Coldebella, Gus P., and Brian M. White. (January 2010): 233-245.
[52] Flowers, Angelyn, and Sherali Zeadally. (June 2014).

Case Studies

Regulating and defending the cyber domain implies a firm understanding of the costs and benefits of applying those regulations in response to defined risks. A recent analysis by Mandiant, detailing Chinese cyber intrusions and the subsequent theft of intellectual property from commercial company networks, emphasizes the urgency of implementing policies and procedures that support the security of U.S. owned cyber systems.[53] To analyze the proposed approaches two case studies are examined to determine if there is reasonable methodology to thwarting or mitigating the effects of cyber enabled attacks. Through analysis, the ideas of state centric regulation, polycentric cooperative governance, and active defense are tested as options against these case studies to determine their validity for combating future incidents.

2013 Target Computer Network Exploitation

The November 2013 computer network exploitation on Target's security payments system was, at the time, the largest breach of customer information in history.[54] Between 27 November and 15 December, hackers suspected to have originated in Russia lifted the credit card information of 40 million Target customers.[55] Further, the company confirmed that the

[53] Mandiant. (February 2013).
[54] Riley, Michael, et al. "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It." Businessweek.Com (March 13, 2014): 1. Military & Government Collection, EBSCOhost (accessed June 20, 2015).
[55] Clark, Meagan. "Timeline of Target's Data Breach and Aftermath: How Cybertheft Snowballed For the Giant Retailer." *International Business Times*. May 5, 2014. http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056 (accessed April 2, 2015).

personally identifiable information (PII) of as many as 70 million customers was stolen.[56] The assessment determined that the likely origination of the hack was stolen credentials of a third party service company.[57]

The malicious activities began with the perpetrators inserting malware into the Target network that has been described as not very sophisticated.[58] Through the use of the exploited credentials the hackers took their time to test their malware on a few of the companies' cash registers before pushing the malware out to most of the retailers' store's point of sale machines.[59] Despite the perpetrators maneuvering the Target network for several weeks, the company did not detect the intrusion.[60] In the end, the Israeli based company Seculert assessed that approximately 11 gigabytes of data were extracted from Target servers.[61]

Target had taken proactive steps to mitigate these types of malicious cyber activities; in fact, six months before the incident they had begun installing cybersecurity tools from FireEye.[62] The inclusion of detection tools in the security suite was designed to detect malware just like that used by the malicious actors.[63] The initial reaction by Target leadership was typical of

---

[56] Weiss, N. Eric, and Rena S. Miller. *The Target and Other Financial Data Breaches: Frequently Asked Questions.* Report, International Security & Counter Terrorism Reference Center, Congressional Research Service, Washington, D.C.: Congressional Research Service, 2014, 1-33: 2
[57] Krebs, Brian. *Target Hackers Broke in Via HVAC Company.* February 5, 2014. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ (accessed April 2, 2015).
[58] McCracken, Harry. *How Target Made Itself a Target for Hackers.* March 15, 2014. http://time.com/23786/target-data-breach/ (accessed April 2, 2015).
[59] Krebs, Brian. (February 5, 2014).
[60] Riley, Michael, et al. (May 5, 2014): 1.
[61] McCracken, Harry. (March 15, 2014): 1.
[62] Riley, Michael, et al. (May 5, 2014): 1.
[63] Ibid: 1.

company responses – to claim standards were followed, insist steps are being taken and that an investigation is underway to determine the facts.[64] What the executive team may not have initially known was that the $1.6 million dollar investment in FireEye had actually worked.[65] In fact, assessments say that had the security team opted to let the security suite automatically block malware, the intrusion would have been thwarted before it even began.[66]

FireEye caught the perpetrators uploading the malware that ultimately acted as the exfiltration tool that moved the stolen data off Target servers to staging servers.[67] When FireEye alerted, the security team in India flagged the alert and notified the Target security operations center in Minnesota.[68] Unfortunately, the alert was not responded to and the mass exfiltration continued.[69] Target executives noted that the company was unaware of the breach until the Justice Department notified them on or near 13 December when there systems discovered the malicious activities.[70]

Following the meeting with the Justice Department, Target hired a third party to investigate and confirm the extent of the incident.[71] Following the assessment, Target privately confirmed the malicious activities on 15 December followed by a public acknowledgment on 19 December.[72]

---

[64] Riley, Michael, et al. (May 5, 2014): 1.
[65] Ibid: 1.
[66] Ibid: 1.
[67] Ibid: 1.
[68] Ibid: 1.
[69] Ibid: 1.
[70] Clark, Meagan. (May 5, 2014).
[71] Ibid.
[72] Ibid.

The Riley article suggests that several factors could have contributed to the failure of the IT security personnel from responding.[73] These factors include a lack of trust for the new FireEye software, an absence of Security Operation Center leadership due to a recent resignation, and failure to follow up on alerts from both the software and its overseas watch floor.[74] Some other factors that may have contributed to the lack of action include distrust in the overseas watch floor personnel, possibly a lack of training on the new FireEye system and proper response options despite the lengthy certification period.[75] Lastly, secure segregation of the Target networks and sub-networks did not appear to be properly configured.[76]

The breach going public is the only incentive Target needed to appear to be interested in tightening up their security. There is generally very little real incentive for companies to admit they have a problem and even less incentive to spend large sums of money to implement change. As the Bloomberg article indicated, the stock of Target really did not suffer following the breach.[77] However, Target did suffer a short-term immediate effect, with a 46 percent dip in sales for the quarter.[78]

The absence of a decline in stock price is not to imply that there will not be severe long-term effects. Overall, Target estimates the cost of the to

[73] Riley, Michael, et al. (May 5, 2014): 2.
[74] Ibid: 2.
[75] Ibid: 2.
[76] Ibid: 4.
[77] Ibid: 3.
[78] Ibid: 3.

date (February 2015) at over $248 million, with a rough estimate of fraudulent charges between $240 million and $2.2 billion.[79] Target has not seen the end with the possibility of further fines by the Payment Cards Industry Council of up to $1.1 billion and a solid 90 lawsuits pending.[80] Further, Target laid off personnel at its headquarters and worldwide as sales dropped.[81] Despite the hack, just a year later Target had returned to its profitable state, surpassing forecasted revenues with a posting of $17.73 billion, which could mean that the economic effects may have already subsided.[82]

2014 U.S. Investigations Services Computer Network Exploitation

The August 2014 computer network exploitation on U.S. Investigations Services LLC (USIS) provides an example of a private organization whose security practices must conform to government standards because of contractual obligations.[83] This case is pertinent because the company breached was the majority provider of federal background checks for security clearances.[84] The USIS breech also had little or no immediate known effects

[79] Weiss, N. Eric, and Rena S. Miller. (2014): 6.
[80] Riley, Michael, et al. (May 5, 2014): 2.
Weiss, N. Eric, and Rena S. Miller. (2014): 6.
[81] Clark, Meagan. (May 5, 2014).
[82] Kedmey, Dan. "Time.com." *Shoppers Just Don't Care About Credit Card Hacks.* November 20, 2014. http://time.com/3595186/target-home-depot-credit-card-hacks/ (accessed April 2, 2015).
[83] Jayakumar, Amrita. *USIS cuts more than 2,500 jobs after losing contracts in wake of cyberattack.* October 7, 2014. http://www.washingtonpost.com/business/capitalbusiness/usis-cuts-more-than-2500-jobs-after-losing-contracts-in-wake-of-cyberattack/2014/10/07/5816cfb2-4e3f-11e4-babe-e91da079cb8a_story.html (accessed April 2, 2015).
[84] Ibid.

from the malicious activities directly relating to the data loss but rather there were immediate and lasting secondary effects to the company.

Despite the government-approved cybersecurity measures including perimeter protection, antivirus, user authentication and intrusion-detection, purported Chinese actors penetrated the companies' networks.[85] Reports suggest that the breech into USIS networks was a state sponsored attempt to steal copies of background investigation files for federal government and federal contract employees.[86] The breech exposed at least 25,000 employee background investigations that reveal in depth personal information.[87] Similar to the JP Morgan Chase event the USIS event went unnoticed by the company for several months.[88] Though USIS reported the incident to the government, once it was noticed USIS delayed reporting the loss to the public for a few more months.[89]

The response to the USIS exploitation by the government was swift. The government suspended and subsequently cancelled contracts for services provided by USIS for services to The Department of Homeland Security

---

[85] Fox News. *Hacker attack on federal security contractor not noticed for months, report claims.* November 4, 2014. http://www.foxnews.com/tech/2014/11/04/hacker-attack-on-federal-security-contractor-not-noticed-for-months-report/ (accessed March 28, 2015).
[86] Paganini, Pierluigi. *The network of USIS compromised by a cyberattack.* August 12, 2014. http://securityaffairs.co/wordpress/27499/cyber-crime/network-usis-compromised-cyber-attack.html (accessed April 1, 2015).
[87] Fox News. (2014).
U.S. Investigations Services. *USIS Comments on Recent Self-Reported Cyber-Attack on Corporate Network.* August 6, 2014. http://www.usis.com/Media-Release-Detail.aspx?dpid=151 (accessed April 2, 2015).
[88] Fox News. (2014).
[89] Ibid.

(DHS) and The Office of Personnel Management.[90] The resulting cancellations caused USIS to lay off 2,500 employees nationwide.[91] The company suffered massive capital loss from the cyber incident. USIS lost an estimated $510 million in business (approximately $320 million from The Office of Personnel Management and approximately and $190 million from The Department of Homeland Security) overnight.[92]

Following the incident, the government chose to shift the business to other contractors and to use in house solutions, moving some of the business to competitor companies such as CACI and KeyPoint Government Solutions.[93] Ironically, KeyPoint suffered a breech in its computer systems in December 2014 that resulted in the exposure of approximately 40,000 federal employee background records. This exposure suggested that government actions to mitigate the breech were ineffective.[94]

Analysis

Polycentric Governance Model

Applying the polycentric governance model to the Target cyber intrusion shows both strengths and weaknesses. The strength of the polycentric governance model in this case is the concept of establishing cyber

---

[90] Medici, Andy. *DHS, OPM suspend contracts with USIS after major cyberattack*. August 7, 2014. http://archive.federaltimes.com/article/20140807/IT/308070009/DHS-OPM-suspend-contracts-USIS-after-major-cyber-attack (accessed March 25, 2015).
[91] Jayakumar, Amrita. (2014).
[92] Fox News. (2014).
Jayakumar, Amrita. (2014).
[93] Jayakumar, Amrita. (2014).
[94] CBS News. *Files of more than 40,000 federal workers breached in cyberattack*. December 18, 2014. http://www.cbsnews.com/news/files-of-more-than-40000-federal-workers-breached-in-cyberattack/ (accessed March 25, 2015).

norms.[95] The polycentric governance argument promotes cyber norms as a method to enlist users that maintain security through best practices. In theory, this would enhance the ability of Target to avoid incidents in the cyber domain though collective action of users outside of their company owned networks. The polycentric approach of collaborative interaction between the government, companies and private citizens argues that Target would benefit from standardization, notification and other defensive measures. The global approach of polycentric governance argues that a multipronged governance structure that includes states, businesses, individuals, and international bodies working to maintain the integrity of the system will enhance the security of companies like Target. This type of structure would benefit the system as a whole.[96]

The polycentric governance theory appears to be a logical approach to a very difficult problem, e.g. preventing Target-type malicious cyber incidents. Where the approach fails is the faith-based application of standards within the collective and the legal pitfalls each member of the collective must identify and mitigate to participate in the voluntary scheme. This view focuses on the interaction between the state and commercial and private actors. In this example, a nonprofessional can determine that there will be severe difficulties in sharing information between government agencies,

---

[95] Brechbuhl, Hans, et al. (January 2010): 83-91.
Hunker, Jeffrey. (2010): 197-216.
[96] Brechbuhl, Hans, et al. (January 2010): 83-91.
DeNardis, L. (2010): 129–164.

companies and private individuals; all have different motivations, legal obligations, and costs to consider.

Further, the global polycentric governance approach exacerbates the previous indigenous polycentric approach by ignoring the extremely complex relationships that must be created to implement a global strategy. Neither of these approaches addresses how they would actually prevent incidents like that at Target from occurring. These approaches also disregard the cost associated with implementing and maintaining even a rudimentary polycentric governance approach. The polycentric approach suggests that the stakeholders would share resources to compound the security interest of each other. Companies and government stakeholders would have to implicitly trust each other and refrain from suing if the resources of one stakeholder damaged another. In a country fraught with litigious actions by individuals, this is an unlikely outcome.

The USIS case is a version of the polycentric governance model focused on the cooperation of the state and the company to provide a method to protect individuals' information. Through contractual language, the government set the behavior norms for the company and the company used approved methodologies to implement and sustain those behavior norms.[97] This model ultimately failed, in part because the company network was used for business beyond that which served the government client. As reported by

[97] Fox News. (2014).

Fox News, the origin of the malicious cyber exploitation event was a weakness in a third party network that had access to the USIS network.[98]

The polycentric governance model should account for this type of connection but the standards currently in place do not account for the diversity in the cyber domain. In response to the recognition of this shortfall, Senator Tom Carper (D-DE) suggested congressional action to pass the Federal Information Security Modernization Act of 2014.[99] Despite the political rhetoric, the implementation of the act promotes real-time automated security measures. The delineation of agency roles does not provide proactive steps to thwart criminals or states from attacking systems; rather this legislature is another attempt to respond in the aftermath of a malicious cyber incident.[100]

The main difference between the Target case and the USIS case is the involvement of the government. In the Target case, the government only acted as a law enforcement entity to provide post facto attempts to prosecute the perpetrators of the theft. In the USIS case, the government was acting as oversight, customer and law enforcement. In neither case does the polycentric governance model appear to be a viable solution to preventing or mitigating malicious cyber activities. Though the analysis shows that there is not a formal polycentric approach to cybersecurity, the concept presented in

[98] Ibid.
[99] Medici, Andy. (2014).
[100] Ibid.

multiple studies suggests that the scenarios that led to the eventual theft in both cases would have played out approximately the same way because the actors perpetrating the malicious cyber activities would not have been part of the cooperative polycentric governance. Without willing compliance of malicious actors to follow rules, the polycentric model is limited in its ability to thwart malicious cyber activities. However, the more willing participants in the governance structure the ability of the collective to blunt incidents and respond more rapidly in times of crisis increases.

State Centric Governance Model

Applying the state centric governance model to the Target computer network exploitation is very difficult because state centric regulation and control does not easily extend to private networks. [101] This model suggests government action through legislation that involves centralizing control over government cybersecurity, improving cyber governance procedures, promoting cyber norms and encouraging private sector participation.[102] The main fault in this argument is the dismissal of the ownership of the cyber domain. Most of the cyber domain, including 85% of the U.S. controlled critical cyber infrastructure, is privately owned. This private ownership

---

[101] Broggi, Jeremy J. (2014): 653-676.
Hunker, Jeffrey. (2010): 197-216.
Newmeyer, Kevin P. (March 2012): 115-126.
U.S. Govt. Accountability Office. (2011).
[102] Broggi, Jeremy J. (2014): 653-676.
Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. (April 2013): 1-27.
Hunker, Jeffrey. (2010): 197-216.
Newmeyer, Kevin P. (March 2012): 115-126.
Shackelford, Scott J, and Amanda N Craig. (2014): 119-184.

includes the Target servers that were infiltrated.[103] The state centric approach implies that the government will provide security through regulation and enforcement. In political terms, this is a great campaign sound bite; however, in practice it is very difficult to implement when the government is unable to secure its own networks. The focus on centralized solutions for an amorphous problem lacks the fluidity required overcoming the evolving cybersecurity challenge. Further, the legal authority to regulate the cyber domain is mired in constitutional protections and difficult-to-navigate laws and regulations.[104] The state centric approach, like the polycentric approach, also fails to suggest how the regulation of the cyber domain by the state will prevent or mitigate cyber intrusions.

The USIS case is one that could benefit from the concept of a state centric governance model. If the federal government was able to centralize control over government cybersecurity, then improving cyber governance procedures and promoting cyber norms private sector participation might actually be achievable.[105] A set of standards to manage networks that are flexible and implementable by all individuals, businesses, and government agencies might actually lead to a defendable network infrastructure. The USIS breech is a case where the stakes of the government and the company

---

[103] Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. (April 2013): 1-27.
[104] Opderbeck, David W. (May 2012): 795-845
[105] Broggi, Jeremy J. (2014): 653-676.
Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. (April 2013): 1-27.
Hunker, Jeffrey. (2010): 197-216.
Newmeyer, Kevin P. (March 2012): 115-126.
Shackelford, Scott J, and Amanda N Craig. (2014): 119-184.

are intertwined in very real and tangible ways. The government desires to maintain the security of personnel records and the company wants to maintain profits. Despite the obvious attempt to work together to meet both of their requirements, the application of the model ultimately failed.

As noted in above, the main difference between the Target case and the USIS case is the involvement of the government. In the Target case, the government only acted as a law enforcement entity to provide post facto attempts to prosecute the perpetrators of the theft. In the USIS case, the government was acting as oversight, customer and law enforcement. The Target case contrasts the USIS case mainly with regard to the quasi-state centric approach the government implemented vis–à–vis contractual obligations. While Target was under regulatory compliance mandates, the contractual obligations placed on USIS in conducting business with the government were more consistent with the state centric approach described in the literature.

Active Defense Model

Applying the active defense model to the Target case is compelling because it implies that while active defense may not have prevented the initial intrusion, an active defense posture would have allowed the government to take action that is more aggressive. [106] If we define deterrence as actions that reduce the cost benefit curve for the adversary, then the idea

[106] Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. (January 2010): 1-24.

of active defense, moving away from passivity and defining the justification for military action in the cyber domain, is the only model that appears to actually provide discouragement of malicious activities.[107] The shortfall in the argument is the focus on the state and its needs. In many cases, the state is much easier to control and manage, but the state does not respond to the needs of companies and individuals.[108] A separate shortfall to active defense is the assumption that our military or government in general, has the capacity and competency to conduct cyber warfare either to retaliate against a malicious actor or to take other proactive measures.

Congruent with the Target case outcome, there is little evidence that an active defense model would have prevented the malicious cyber activities on USIS. However, unlike the Target incident, the justification for military action in the cyber domain could be more readily argued in the USIS case because the information stolen is U.S. Government property. The U.S. government, concurrently with the individuals affected, has a legal claim to the information that the malicious actors acquired. Thus, the damage caused to the state could provide legal justification for offensive or retaliatory action. The breadth of action would then be defined through the active defense model and applied in cases such as this.

---

[107] Flowers, Angelyn, and Sherali Zeadally. (June 2014).
Hunker, Jeffrey. (2010): 197-216.
Schwitz, John G. (March 2011): 115-125.
[108] Coldebella, Gus P., and Brian M. White. (January 2010): 233-245.

The contrast between the two cases once again falls to the role of the government. While the Target case reflects very little direct government equity, there is potential damage to Target's market share. In the context of protecting national security, however, one could make an argument that the potential damage might warrant active defense measures by the government, or in this case by Target, in order to prevent possible damage to the U.S. economy and Target assets.

Conclusion

In a perfect world, the polycentric approach to governance would be ideal because the model suggests that everyone with equity in the cyber domain willingly commits to a security and conduct framework. Further, the failure to meet the standards of the framework places overwhelming pressure on the non-compliant actor and/or deters non-compliance from the outset. However, without the willing compliance of malicious actors, the polycentric model is limited in its ability to thwart malicious cyber activities. This approach counts on willing participants to increase the ability of the collective to blunt malicious cyber activities and respond more rapidly.[109]

The state centric approach, at face value, appears to be a reasonable approach to governance given that the state is the normal body of governance. However, the lack of jurisdiction over the basic sundries that comprise the governed structure suggests that the concept of a state centric

[109] Brechbuhl, Hans, et al. (January 2010): 83-91.

approach will not work.[110] Further, the risks that state centric approaches introduce into the global governance process may even lead to further conflict. In a global model with each state attempting to carve out a piece of an amorphous domain to reign, the potential for conflict is high.

The active defense model is perhaps the most disconcerting because the term 'defense' implies a non-aggressive approach to implementing self-protection measures. However, the implication is that through active defense the perpetrator would suffer some sort of damage should they attack a protected enclave.[111] The potential for this type of governance to spin out of control is high because there is very little understanding of the consequences of both the initial attack and the active defense response activities.

One other option not explored in this chapter is a purely private governance process. This governance process would be one that leaves the states completely out of the decision-making tree, and compels individuals and companies to set standards of conduct on the Internet. More work could be done to investigate the potential impacts of this kind of governance; however, it is outside the scope of this chapter.

Perhaps the best model for governance is a combination of all of these models. In the short term, the best plan may be to keep all options on the

---

[110] Chinn, David, James Kaplan, and Allen Weinberg. "Risk and responsibility in a hyperconnected world." *McKinsey.com*. January 2014. http://www.mckinsey.com/~/media/mckinsey/dotcom/insights/business%20technology/risk%20and%20responsibility%20in%20a%20hyperconnected%20world%20implications%20for%20enterprises/risk%20and%20responsibility%20in%20a%20hyperconnected%20world.ashx (accessed March 2, 2015).

[111] Flowers, Angelyn, and Sherali Zeadally. (June 2014).

table. The continual evolution of the global commons in complexity compels changes to the underlying security infrastructure. As previously mentioned, the Internet was never designed to be secure. The solution may need to be a fundamental change to the base structure of the Internet that provides the security necessary in a world where the technology driving forward innovation and growth is the same one that may be the vehicle to cause the next world war.

Chapter 2: Economic Impacts of Malicious Cyber Incident Response

Introduction

This chapter serves to explore the threat to the United States economy through malicious cyber activities. Recent known cyber incidents at JP Morgan Chase and Sony are examined to compare the government response in each incident. The government response to the Sony cyberattack (which had a estimated cost of $35 million) appears to have been an over reaction by the government. In contrast, the JP Morgan Chase cyber exploitation (which had a estimated of $20 million) appears to have been an under reaction because of the greater threat to the U.S. economy in the JP Morgan Chase cyber exploitation. Next, the chapter presents a literature review, then explores each case, concluding that given the relative threat to the economy there appeared to be a failure to properly evaluate the relative risk to national security; the response to the two malicious cyber incidents was opposite of what should have been expected.

The scale and impact of malicious cyber events has increased with the proliferation of the Internet. These incidents generally result in the theft of information such as proprietary industrial processes, intellectual property, personal information, military and government secrets, and business confidential information including sensitive contract negotiation data. In some instances, however, there is intentional damage done to the attacked

network.[112] Generally, this results in the damage of networks though the erasure of information. These malicious activities can cause the compromised network to become unusable in the absence of significant reconstitution or replacement.

There is varying opinion regarding the value of the information stolen though these computer network exploitation activities, as well as the cost to recover, mitigate and stop the activities from continuing.[113] Some leaders have even described the current state of affairs as the "greatest transfer of wealth in history."[114] In a recent survey of private industry incidents, respondents estimated costs between $6.3 million and $8.4 million a day just for the down time incurred.[115] However, these figures only consider a non-

---

[112] Sicard, Sarah. "North Korean Cyberattack on Sony Poses Tough Security Questions." National Defense 99, no. 736 (March 2015): 24-25.

[113] Bauer, Johannes M., and Michel Van Eeten. "Introduction to the Economics of Cybersecurity." *Communications and Strategies*, no. 81 (1st Quarter 2011): 13-21.
Cashell, Brian, William D. Jackson, Mark Jickling, and Baird Webel. *The Economic Impact of Cyber-Attacks.* Report, Government and Finance Division, Congressional Research Service, Washington, D.C.: Congressional Research Service, 2004.
Center for Strategic and International Studies. "The Economic Impact of Cybercrime and Cyber Espionage." *Center for Strategic and International Studies.* July 2013. http://csis.org/publication/economic-impact-cybercrime-and-cyber-espionage (accessed March 2, 2015).
Center for Strategic and International Studies. "Net Losses: Estimating the Global Cost of Cybercrime." *Center for Strategic and International Studies.* June 2014. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf (accessed May 9, 2015).
Oxford Economic. "Cyber-attacks: Effects on UK Companies." *Oxford Economic.* July 2014. http://www.cpni.gov.uk/documents/publications/2014/oxford-economics-cyber-effects-uk-companies.pdf?epslanguage=en-gb (accessed May 9, 2015).
Ponemon Institute. "2014 Cost of Cyber Crime Study: United States." *Ponemon Institute.* October 2014. http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf (accessed March 2, 2015).
Ponemon Institute. "2014 Global Report on the Cost of Cyber Crime." *Ponemon Institute.* October 2014. http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/ (accessed June 5, 2015).
Roberts, Paul F. and Paul Kielstra. "Measuring the cost of cybercrime." *The Economist.* Edited by Riva Richmond. May 20, 2013. http://www.economistinsights.com/technology-innovation/analysis/measuring-cost-cybercrime (accessed June 5, 2015).
Taylor, Brian. "Cyberattacks fallout could cost the global economy $3 trillion by 2020." *Tech Republic.* February 20, 2014. http://www.techrepublic.com/article/cyberattacks-fallout-could-cost-the-global-economy-3-trillion-by-2020/ (accessed March 2, 2015).

[114] Rogin, Josh. *The Cable.* July 9, 2012. http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history (accessed 10 19, 2013).

[115] McAfee. (December 29, 2010).

destructive incident. The damages done in destructive cyberattack incidents do not yet have an adequate model for accurately measuring the economic impact to the attacked entity or the ripple effect to the local, regional and global economy. [116]

Despite the source of opinion, the consensus is that malicious cyber incidents, regardless of the information stolen or damages incurred, cost billions of dollars each year. Further, the number of people directly or indirectly affected by cyber theft increases with each incident.[117] In only one of the cases examined, malicious cyber exploitation on JP Morgan Chase the total number of households and businesses affected topped 80 million.[118] This incident is recognized as one of the largest computer network exploitation breaches ever discovered.[119] What the reports about this and other incidents sometimes fail to adequately describe is that using 80 million as a metric does not fully express the severity of the incident. For each business and household affected, 76 million and seven million respectively, there are between one and hundreds, if not thousands, of people and other businesses affected, as second and third order effects.[120]

If the current assessments of the relative costs of these incidents are correct, and the number of people affected by these malicious cyber activities

---

[116] Center for Strategic and International Studies. (June 2014).
[117] Center for Strategic and International Studies. (March 2014).
[118] Rushe, Dominic. "JP Morgan Chase reveals massive data breach affecting 76m households." *The Guardian.* October 3, 2014. http://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach (accessed April 5, 2015).
[119] Ibid.
[120] Silver-Greenberg, Jessica and Matthew Goldstein. "After Breach, Push to Close Security Gaps." *The New York Times.* October 22, 2014. (accessed March 2, 2015).

approaches the hundreds of millions, the question remains: why is the public and government reaction to these malicious cyber incidents so lackluster?[121] Is there a failure in the assessments regarding cyber theft as a threat to the economy? The reason for the lack of a coherent consistent approach to these events is most likely caused by a multitude of complex factors that are situation and time dependent. One of the more prominent factors that likely cause the government to react is the presence or absence of public concern. However, using public concern as a metric for determining what actions the government should take does not capture the complexity of either the JP Morgan Chase computer network exploitation or the Sony cyberattack.

As we consider what impact malicious cyber activities have on the economy it is easy to focus on the issue through the lens of monetary cost, e.g. cost to companies and individuals in the form of loss through theft, damages, potential revenue losses, increased competition and other impacts. It is much more difficult to consider malicious cyber activities as a potentially serious threat to the stability of the U.S. economy. Despite the abstract nature of the cyber threat, there are weaknesses in the economic system, which, if enacted upon, could have far reaching effects. The government has responded to similar threats to the stability of the economy in the past. During the 2008 economic crisis, the U.S. government reacted by providing massive

[121] Center for Strategic and International Studies. (July 2013).
Ponemon Institute. (October 2014).
Oxford Economics. (July 2014).

government aid to banking institutions.[122] By some assessments, without intervention there would have been a much more severe effect on the U.S. economy, and, as a reflection, the global economy.[123]

Literature Review

There is a vast body of opinions regarding how the government should respond to malicious cyber activities. In the last fifteen years in particular, the government has increased its level of attention on the issue of malicious cyber activities, on not only government and military systems, but private industry as well. This expansion of attention suggests that there is a consensus regarding when the government should take action. In fact, there are many ideas regarding how to govern the Internet and those governance types each suggest different responses.

This literature review helps identify some of the ideas that resonate in the literature regarding the appropriate response to malicious cyber activities. The review focused on themes that capture ideas about the proper response to cyber incidents that are a risk to national security and in particular those cyber incidents that could have disruptive effects for the economy. Where possible, the literature review attempts to show the most common suggested responses to malicious cyber activities. To limit the review to a reasonable number of ideas they have been binned into three overarching

---

[122] Reyes, Anthony. "The Financial Crisis Five Years Later: Response, Reform, and Progress in Charts." U.S. Treasury. September 2013. http://www.treasury.gov/connect/blog/Documents/FinancialCrisis5Yr_vFINAL.pdf (accessed June 7, 2015).
[123] Ibid.

categories that help manage the concepts. These concepts are used to model the possible governance approaches where they might suggest ways to stop and respond to malicious cyber activities.

Polycentric Response Approach

There are multiple viewpoints regarding how to manage response to malicious cyber activities the Internet. One of the most discussed ideas to respond to malicious cyber activities is polycentric governance.[124] Polycentric responses accept the heterogeneous nature of the cyber domain. This type of response approach assumes cooperative actions by individuals, states, and international bodies in part because none have full ownership or management over the entire domain.[125] This response model is consistent with the current ownership of the Internet.

The polycentric governance model suggests that malicious cyber incident response would be best through cooperative actions based on pre-negotiated rules and standards that establish the behavior norms that define acceptable and unacceptable behavior.[126] The concept is based on the idea that through the development of cyber norms, Internet users will maintain security through best practices and cyber incident responses would be a

---

[124] Brechbuhl, Hans, et al. (January 2010): 83-91.
Contreras, Jorge L., Laura Denardis, and Melanie Teplinsky. (June 2013): 1113-1130.
Shackelford, Scott J. (June 2013): 1273-1364.
[125] Defense Science Board. (January 2013).
[126] Brechbuhl, Hans, et al. (January 2010): 87.
Hunker, Jeffrey. (2010): 197-216.
Shackelford, Scott J. (June 2013): 1273-1364.

multi-vector group effort. The importance of private industry in this type of response model is acknowledged when looking at a polycentric model.[127]

Some of the studies focus on polycentricism within the state itself.[128] These studies look at interaction between the state and commercial or private actors in regulating the Internet. The model presents a view where malicious cyber incidents are responded to in a collaborative effort with representatives from the government and interested industry parties to determine a resolution. In this concept, the model accepts a relationship between the state and private industry that is required to respond to complex incidents. The model suggests that through the division of labor the state and the private sector can respond more effectively. Some even suggest that the lead for cybersecurity in many instances is industry, with the state serving only in a limited role.[129] Regardless of the exact approach in executing the polycentric response approach, cooperation amongst the various members of the response team is paramount.

In other examples of polycentric approaches, the multipronged governance structure accounts for the global nature of the cyber domain by suggesting that states, businesses, individuals, and international bodies must work together to maintain the integrity of the system.[130] This approach

---

[127] Farwell, James P. "Industry's Vital Role in National Cyber Security." *Strategic Studies Quarterly* (International Security & Counter Terrorism Reference Center) 6, no. 4 (Winter 2012): 10-41.
[128] Broggi, Jeremy J. (2014): 653-676.
Contreras, Jorge L., Laura Denardis, and Melanie Teplinsky. (June 2013): 1113-1130.
Hunker, Jeffrey. (2010): 197-216.
[129] Farwell, James P. (Winter 2012): 10-41.
[130] Brechbuhl, Hans, et al. (January 2010): 83-91.

expands the polycentric governance model to a larger global scale through bilateral and multilateral security and conduct agreements. This model looks to respond to malicious cyber incidents through the enforcement of rules and laws.[131]

The strength of the polycentric approach is acceptance of plurality of ownership, the lack of defined borders and boundaries, and the complexity of the interconnectedness of the cyber domain, all of which provide a wide variety of cyber incident response options.[132] The expanded nature of the governance model would also broaden the proliferation of cybersecurity solutions to all stakeholders. Through cooperation, this model suggests a strength-in-numbers approach. This appears to be a relevant approach, assuming all of the stakeholders have the same priorities.

Multipronged or polycentric governance response modes downplay the difficulty of resolving complex issues with multiple stakeholders of varying motivations. Because of these complexities some of the literature suggests that traditional regulatory and legal procedures will not work.[133] This would in turn limit any possibilities for cyber incident response and, without a new

---

DeNardis, L. (2010): 129–164.

[131] Newmeyer, Kevin P. (March 2012): 115-126.

[132] Contreras, Jorge L., Laura Denardis, and Melanie Teplinsky. (June 2013): 1113-1130.

[133] Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. (January 2010): 1-24.
Malone, Eloise F., and Michael Malone. (August 2013): 158-177.
Ferraro, Matthew F. "Groundbreaking" or broken? An analysis of SEC Cybersecurity disclosure guidance, its effectiveness, and implications." *Albany Law Review* (Academic Search Complete, EBSCOhost (accessed June 28, 2015).) 77, no. 2 (April 2014): 297-347.
Inserra, Paul Rosenzweig and David. *Government Cyber Failures Reveal Weaknesses of Regulatory Approach to Cybersecurity*. June 13, 2013. http://www.heritage.org/research/reports/2013/06/weaknesses-of-a-regulatory-approach-to-cybersecurity (accessed April 3, 2015).

form of regulating that is able to come to a consensus on priorities, the idea of polycentric or multipronged governance may not be viable.[134]

State Centric Response Approach

These solutions seek government action through legislation that involves centralizing control over government cybersecurity, improving cyber governance procedures, promoting cyber norms and encouraging private sector participation with a government lead.[135] This approach assumes that through regulation the needs for cyber incident response will decrease through deterrence.

State centric response approaches focus on managing cyber incidents on state controlled networks and the extension of state controlled response mechanisms to the private sector in emergencies.[136] The state centric approach implies that state controlled networks are of higher priority for response that the security of critical infrastructure owned by private industry. This approach does not present reasonable response options because most of the critical infrastructure resides on private networks. Rather, these approaches look to developing methods to defend state controlled networks in an attempt to manage critical nodes.

---

[134] Contreras, Jorge L., Laura Denardis, and Melanie Teplinsky. (June 2013): 1113-1130.
[135] Broggi, Jeremy J. (2014): 653-676.
Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. (April 2013): 1-27.
Hunker, Jeffrey. (2010): 197-216.
Newmeyer, Kevin P. (March 2012): 115-126.
Shackelford, Scott J, and Amanda N Craig. (2014): 119-184.
[136] Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. (January 2010): 1-24.
Hunker, Jeffrey. (2010): 197-216.

While there have been multiple proposals for making this achievable, to date, the concept is still very difficult to implement.[137] This approach is an attempt to provide response options through the centralization of command and control for government networks such as the Department of Homeland Security, the State Department, and the Defense Department. Because numerous stakeholders want to maintain control over their individual networks the implementation of standardized security practices by governments can be difficult.[138]

In theory, a centralized government cybersecurity response structure for would enable the government to respond to cyber incidents more efficiently. However, this approach also reduces the control of the individual stakeholders such as the State Department or Defense Department over their own networks. The state centric response model also has one major shortfall because it ignores the interconnectedness of the private sector with its networks though partnerships, contracts, and physical infrastructure.

State centric governance writings are strong in their assessment of the government to manage cyber incident response for state controlled networks. [139] The literature acknowledges some of the difficulties of responding to cyber incidents specifically with regard to ownership of the

---

[137] DeNardis, L. (2010): 129–164.
Klimburg, Alexander. (2012).
[138] U.S. Govt. Accountability Office. Cyberspace: United States Faces Challenges In Addressing Global Cybersecurity and Governance. (2010).
[139] Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. (April 2013): 1-27.
Greenwald, Eric A. (January 2010): 41-62.
Heilbrun, Mark R., and Isaac Brown. (December 2011): 14-20.

Internet structure. Through the recognition of the difficulties the literature attempts to narrow response options to specific portions of the Internet. Limiting the response options to specific sets of the Internet allows the authors to present methods for responding to cyber incidents.[140]

The shortfalls in these writings with regard to response modeling is a lack of inclusion of various risk factors such as international laws, the needs of multiple sovereign states and the continuously evolving structure of the Internet. They also lack an appreciation for the fact that centralized solutions will be difficult to implement in an amorphous domain.

Active Defense Response Approach

One of the more compelling response options is the active defense approach. This model manifested in different ways. In some the response option presented options for proactive retaliation against a malicious actor, while other options suggested diverting a malicious actor to a controlled network. Other ideas postulated setting cyber deterrence aside and adopting a full war-fighting posture.[141] Each of these ideas presented methods for responding to cyber incidents in a much more proactive manner than those presented in the polycentric or state centric response approaches. The active defense approach looked more toward moving to a war-fighting posture in the

---

[140] Contreras, Jorge L., Laura Denardis, and Melanie Teplinsky. (June 2013): 1113-1130.
Flowers, Angelyn, and Sherali Zeadally. (June 2014).
Hunker, Jeffrey. (2010): 197-216.
[141] Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. (January 2010): 1-24.

cyber domain and searching for a way to define the justification for military action in the cyber domain.[142]

This approach in a response model appears rational given the potential negative effects of malicious cyber incidents. One of the more complex problems with this approach is the lack of precedent for the conduct of war in the cyber domain.[143] Current cyber defense, cyber strategy and cyber policy, the doctrine, training, methodologies, tactics, techniques and procedures are far from perfected which lends to multiple problems in implementing an active defense posture.[144] Some of the literature even suggests that active defense response activities could be more detrimental to the defender than the attacker. Active defense responses are easily misconstrued as attacks rather than defense, potentially escalating the event further, even risking actions spilling over the physical world.[145]

The active defense argument has some strengths in driving the conversation of response options. One of those is identifying a need to categorize malicious activities in a way that allows for building response options ahead of time. These options would have to be built to respond in a manner appropriate for the risk and damage the malicious cyber activity may

---

[142] Flowers, Angelyn, and Sherali Zeadally. (June 2014).
Hunker, Jeffrey. (2010): 197-216.
Kesan, Jay P., and Carol M. Hayes. (Spring 2012): 415-529.
Schwitz, John G. (March 2011): 115-125.
[143] Glenny, Misha, and Camino Kavanagh. "800 Titles but No Policy—Thoughts on Cyber Warfare." *American Foreign Policy Interests* (Academic Search Complete) 34, no. 6 (November 2012): 287-294.
[144] Department of Defense. (July 2011).
Department of Defense. (November 2011)
[145] Defense Science Board. (January 2013).
Flowers, Angelyn, and Sherali Zeadally. (June 2014).

cause. In the active defense model the state and its needs, which in many cases is much easier to control and manage are more prominent but the model must also account for private requirements as well.[146] The main shortfall in an active defense that is state centric are the implications of hardening government-controlled networks without finding a way to help the private infrastructure those networks ride on.[147]

Case Studies

The case studies presented were selected to gauge the reactions of the general populous, the U.S. government, and the private sector. The cases were chosen to represent two different types of events. The 2014 Sony event represents a suspected attack on a publically traded company with an apparent attempt to coerce Sony leadership to take specific actions. In contrast, the 2014 JP Morgan Chase incident resulted in the apparent theft of millions of customers' account and personal information. Each case is examined to determine what the consequences of the incident are and the subsequent actions the companies and the government took to respond to those incidents.

2014 Sony Cyberattack

The November 2014 cyberattack on Sony was not the first the company experienced. However, this cyberattack was one that Sony, the U.S.

---

[146] Coldebella, Gus P., and Brian M. White. (January 2010): 233-245.
[147] Flowers, Angelyn, and Sherali Zeadally. (June 2014).

Government and the public would see as a new level of threat.[148] The level of penetration by the perpetrators became apparent to Sony, the FBI and, consequently, the public when the hackers began systematically stealing data and crippling the remains of Sony's computer networks. The hackers also issued threats to Sony employees and the public through targeted emails.[149]

Even before the attacks were known, the FBI asserts the hackers had been on Sony networks for more than two months.[150] During this time, the FBI states that the hackers conducted network mapping and preparation activities that allowed them to ex-filtrate roughly 100 terabytes of information during the final attack phase.[151]

The attacks were detected by the FBI in late November and subsequently revealed a severe breach of the Sony network, as well as the theft of terabytes of data, including business communications, movies, and personal information for employees and celebrities. [152] Following the intrusion, Sony contacted the FBI to inform them of the incident, which did not initially draw serious concern on the part of the government.[153] Shortly after the notification of the FBI, the attackers leaked the stolen information in an apparent attempt to harm Sony. The attackers began the leaks through

---

[148] Elgan, Mike. "Why the Sony Hack Is the Start of Endless Cyber-War." Eweek. December 29, 2014: 1.
[149] Risk Based Security. *A Breakdown and Analysis of the December, 2014 Sony Hack.* December 5, 2014. www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/ (accessed June 4, 2015).
[150] Shaw, C. Mitchell. "FBI Wrong on Sony Hack." *New American* 31, no. 4 (February 2015): 22-25.
[151] Ibid.
[152] Elgan, Mike. (December 29, 2014): 1.
[153] Devlin, Barrett and Danny Yadron. "Sony, U.S. Agencies Fumbled after Cyberattack; Lack of Information and Consultation Led to Flip-Flops, Confusion." *The Wall Street Journal.* February 22, 2015. http://search.proquest.com/docview/1657238447?accountid=11752. (accessed March 2, 2015).

the release of several movies, and continued with batch releases of information on 1 December and 3 December.[154] Just before the third release of information, the FBI was able to confirm threatening emails sent to Sony personnel from the purported perpetrator of the cyberattacks, North Korea.[155]

By Thursday, 18 December, the White House issued a statement indicating that the President was taking the incident as a serious matter and that the U.S. government may be conducting a response with proportional effect.[156] This announcement was just days after a related anonymous threat was released that proposed 9-11 style attacks on movie theaters if they screened the Sony produced movie *The Interview.*[157] Further, the government took cooperative actions such as seeking assistance from the Chinese government and issuing sanctions against North Koreans.[158]

The government response was described as unprecedented, despite contrasting views on the actual economic impacts of the attacks. Some experts pegged the costs to Sony in the $100 million dollar range while the CEO of Sony assessed the costs would be closer to $35 million dollars.[159]

---

[154] Risk Based Security. (December 5, 2014).
[155] Laughland, Oliver and Dominic Rushe. "Sony cyberattack linked to North Korean government hackers, FBI says." *The Guardian.* December 19, 2014. http://www.theguardian.com/us-news/2014/dec/19/north-korea-responsible-sony-hack-us-official (accessed March 2, 2015).
[156] Brunnstrom, David and Jim Finkle. "U.S. considers 'proportional' response to Sony hacking attack." *Reuters.* December 18, 2014. http://www.reuters.com/article/2014/12/19/us-sony-cybersecurity-northkorea-idUSKBN0JW24Z20141219 (accessed March 2, 2015).
[157] Devlin, Barrett and Danny Yadron. (February 22, 2015).
[158] BBC. "Sony cyber-attack: North Korea faces new US sanctions." *BBC.* January 3, 2015. http://www.bbc.com/news/world-us-canada-30661973 (accessed April 5, 2015).
[159] Ando, Ritsuko. "Sony CEO sees no major financial impact from cyberattack." *Reuters.* January 6, 2015. http://uk.reuters.com/article/2015/01/06/uk-sony-cybersecurity-idUKKBN0KF1ZH20150106 (accessed June 21, 2015).

Following the announcement of the attacks, Sony stock experienced a minor drop of .43%. Despite the immediate monetary effects, the losses were mostly recovered within a couple months.[160]

2014 JP Morgan Chase Computer Network Exploitation

In 2014, JP Morgan Chase was the victim of a malicious computer network exploitation that breached and exploited their corporate network. According to reports, the JP Morgan Chase breach was one of the largest ever reported.[161] The *Wall Street Journal* reported that the breach affected roughly 76 million households and 7 million businesses.[162] One of the notable features of this security breach is the timeline of the incidents that took place. There was roughly a two-month lag from when the security breach was detected, to the time JP Morgan Chase identified the problem, to when they were able to stop it. In brief, the intrusion began in mid-June 2014 when nefarious actors accessed servers containing customer contact information.[163] The perpetrators maintained persistent access to the servers until mid-

---

Lemos, Robert. "Sony Pegs Initial Cyber-Attack Losses at $35 Million." *Eweek.com*. February 4, 2015. http://www.eweek.com/security/sony-pegs-initial-cyber-attack-losses-at-35-million.html (accessed March 12, 2015).
Mamiit, Aaron. "Sony Pictures Cyberattack May Cost $100 Million, Says Expert." *Tech Times*. December 10, 2014. http://www.techtimes.com/articles/21869/20141210/sony-pictures-cyber-attack-may-cost-100-million-says-expert.htm (accessed March 2, 2015).
Sha, Sooraj. "Will Sony really see no financial impact from cyber-attack?" *Computing*. January 8, 2015. http://www.computing.co.uk/ctg/news/2389309/will-sony-really-see-no-financial-impact-from-cyber-attack (accessed June 2, 2015).

[160] Risk Based Security. (December 5, 2014).

[161] Rushe, Dominic. (October 3, 2014).

[162] Glazer, Emily. *J.P. Morgan's Cyberattack: How the Bank Responded*. October 3, 2014. http://blogs.wsj.com/moneybeat/2014/10/03/j-p-morgans-cyber-attack-how-the-bank-responded/ (accessed April 5, 2015).

[163] Glazer, Emily. (October 3, 2014).
Roman, Jeffrey. "JPMorgan Confirms Cyber-Attack." *Bank Info Security*. September 15, 2014. http://www.bankinfosecurity.com/jpmorgan-a-7319 (accessed March 2, 2015).

August, by some accounts gaining access to and stealing gigabytes of sensitive information.[164] Other reports insist that the malicious actors were stopped before they could remove customer data from servers but not before removing files containing information that could possibly help breach the system in the future.[165]

Before JP Morgan Chase intervened, reports indicate the malicious actors infiltrated roughly 90 servers.[166] When JP Morgan Chase recognized the network breach, they directed additional resources to deny continued access. Glazer reported that the response team assembled by JP Morgan Chase included 20 bank executives and roughly 200 personnel in the technology and cybersecurity team.[167] Despite the tenacious efforts by the JP Morgan Chase cybersecurity team, it took several weeks to completely block the malicious activities on their network.[168] Finally, at the end of August, JP Morgan Chase announced that it was working with law enforcement to investigate the incident. Despite several assessments that point to indicators of Russian activities, as of late 2014 there is still no concrete evidence that identifies the perpetrators.[169]

---

[164] Glazer, Emily. (October 3, 2014).
Rushe, Dominic. (October 3, 2014).
[165] Goldstein, Matthew, Nicole Perlroth, and David E. Sanger. *Hackers' Attack Cracked 10 Financial Firms in Major Assault.* October 3, 2014. http://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-assault/?_r=0 (accessed April 4, 2015).
[166] Glazer, Emily. (October 3, 2014).
[167] Ibid.
[168] Goldstein, Matthew, Nicole Perlroth, and David E. Sanger. (October 3, 2014).
[169] Logiurato, Brett. "REPORT: 'Russians' Behind Huge JPMorgan Cyberattack." *Business Insider.* October 4, 2014. http://www.businessinsider.com/jpmorgan-cyber-attack-russian-breach-sanctions-2014-10 (accessed March 2, 2015).
Munoz, Eduardo. *JPMorgan hack exposed data of 83 million, among biggest breaches in history.* October 2, 2014. www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003 (accessed April 5, 2015).
Goldstein, Matthew, Nicole Perlroth, and David E. Sanger. (October 3, 2014).

The incident, like others in recent times, prompted several immediate effects. The first notable effect was the forcing of JP Morgan Chase to reallocate significant resources to stopping the malicious actors.[170] This is a relevant factor because the breach took place despite JP Morgan Chase employing approximately 1,000 people and investing roughly $250 million per year on cybersecurity.[171] As previously noted, the bank redirected a significant percentage of their cybersecurity and executive team to specifically attend to this cyber breach.[172] Part of that response team was dedicated to attempting to attribute the malicious activities to the perpetrator.[173]

Following JP Morgan Chase's announcement of the breach, the company's stock also took a slight hit, falling 0.89%; in today's dollars and company value, this equates to a roughly $20 million loss.[174] While not a substantial figure, considering their market capitalization of $225.45 billion there is potential for a significant market reaction.[175] One of the factors that likely reduced market reaction was, unlike previous malicious cyber exploitations on other institutions such as Target and Home Depot, the data

---

[170] Glazer, Emily. (October 3, 2014).
[171] Rushe, Dominic. (October 3, 2014).
[172] Glazer, Emily. (October 3, 2014).
[173] Robertson, Jordan Robertson and Michael Riley. "JPMorgan Goes to War." *Bloomberg BusinessWeek.* February 19, 2015. http://www.bloomberg.com/news/articles/2015-02-19/jpmorgan-hires-cyberwarriors-to-repel-data-thieves-foreign-powers (accessed March 2, 2015).
[174] Rushe, Dominic. (October 3, 2014).
[175] Marketwatch. *JPMorgan Chase & Co.* April 7, 2015. http://www.marketwatch.com/investing/stock/jpm (accessed April 7, 2015).

breach incurred did not include financial records but rather customer contact information.[176]

Analysis

The limited data for examples of government response to malicious cyber incidents, much of which might be attributed to the infancy of the Internet, increases the challenge to identify which of the response options, if any, may be effective. This expansion of attention to malicious cyber incidents suggests that there is a consensus regarding when the government should take action. This assumption is far from correct, as the complexities of each incident, including the perpetrator and the systems affected, change the potential effects and the possible response options because of multiple legal issues. [177]

Response in a Polycentric Model

The Sony and JP Morgan Chase cases provide evidence of contrasting responses by the government. In the case of Sony, the response by the company focused on saving its reputation and maintaining the ability to conduct business.[178] In this respect, the JP Morgan Chase response was similar. One difference in Sony's response is the limited focus by Sony to attribute the attack to its perpetrator.[179] One reason Sony did not have to respond in the same way resonated from the response of the U.S.

[176] Rushe, Dominic. (October 3, 2014).
[177] Opderbeck, David W. (May 2012): 807
[178] Risk Based Security. (December 5, 2014).
[179] Robertson, Jordan Robertson and Michael Riley. (February 19, 2015).

government. In the Sony case, the government responded very quickly, indicating attribution to the North Korean government and publically condemning them for the attack.[180] The government even went so far as to suggest they would take proportional response actions against North Korea.[181]

In direct contrast, the government responded to JP Morgan Chase in an almost hostile manner. JP Morgan Chase, looking to maintain its reputation, notified the government of the incident. The government sent two teams of FBI personnel to assist in the investigation: one that specialized in criminal exploitation and one specializing in nation–state attacks.[182] JP Morgan Chase and the FBI looked to attribute the incident to a perpetrator, looking both for indicators of criminal and state sponsored malicious activities.[183] Very quickly, the FBI decided that the malicious activities were conducted by criminal actors and discontinued the support of the nation-state specialized team.[184] Despite the danger to the economy, there was no strong public condemnation of the perpetrators by the government.

In the Sony case, the company appeared to embrace the polycentric approach. They worked with the government and the government was active

---

[180] BBC. (January 3, 2015).
[181] Brunnstrom, David and Jim Finkle. (December 18, 2014).
Sanger, David E., Michael S. Schmidt and Nicole Perlroth. "Obama Vows a Response to Cyberattack on Sony." *The New York Times*. December 14, 2014. http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html (accessed March 12, 2015).
[182] Glazer, Emily. (October 3, 2014).
Robertson, Jordan Robertson and Michael Riley. (February 19, 2015).
[183] Robertson, Jordan Robertson and Michael Riley. (February 19, 2015).
[184] Ibid.

in taking a leadership position to defend the company. The government indicated that the reason they approached the situation with the level of attention they did was due to the threats made by the perpetrator that attempted to suppress the rights of Sony.[185] The President even went so far as to sign an executive order to expand response options, including sanctions, in cases such as the Sony attack.[186] In some ways, the government even stretched the polycentric approach model by seeking help from China to pressure the North Korean government.[187] The inclusion of China into the government response model is consistent with previous policy such as the International Strategy for Cyberspace.[188]

Response in a State Centric Model

In both the Sony and the JP Morgan Chase events, the government worked in a cooperative model; however, there were indicators that Sony believed the government was the lead or preferred a more active leadership

---

[185] Haggard, Stephan, and Jon R. Lindsay. "North Korea and the Sony Hack: Exporting Instability Through Cyberspace." *Asiapacific Issues*, no. 117 (May 2015): 1-8.
Nakashima, Ellen. "Why the Sony hack drew an unprecedented U.S. response against North Korea." *The Washington Post*. January 2015. http://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html (accessed April 23, 2015).
Sanger, David E., Michael S. Schmidt and Nicole Perlroth. (December 14, 2014)
[186] Executive Office of the President of the United States. "Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea"." *Whitehouse.gov*. January 2, 2015. https://www.whitehouse.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s (accessed March 2, 2015).
Melnik, Tatiana. "New U.S. Sanctions Program Seeks to Give Government an Extra Tool to Fight Cyber-Attacks." *Journal of Health Care Compliance* (Business Source Complete) 17, no. 3 (May 2015): 53-56.
[187] Ellis, Ralph, Holly Yan and Kyung Lah. "U.S. seeks China's help against North Korean cyberattacks." *CNN*. December 20, 2014. http://www.cnn.com/2014/12/20/world/asia/north-korea-sony-response/ (accessed March 2, 2015).
[188] Executive Office of the President of the United States. "International Strategy for Cyberspace." *www.whitehouse.gov*. May 2011. www.whitehouse.gov (accessed September 15, 2013).
Executive Office of the President of the United States. (2010).

role in the responses.[189] Neither case was a solid example of a state centric response.

Response in an Active Defense Model

Only in the Sony attack was there a suggestion of retaliation. Retaliation is not necessarily reflective of an active defense; rather, an active defense suggests methods to mitigate attacks while they are in progress by using active measures against the attacker.[190] Threats of retaliation are closer to conflict escalation activities. Only in the Sony case would an active defense model seem relevant. In this case, attribution was determined: a clear criterion necessary to conduct active defense actions.[191]

Conclusion

Each of the case studies appears, at face value, to represent a similar monetary loss to the companies affected ($20 and 30 million). The threat those losses pose to the economy should demand similar responses from the government and the companies involved in the response. The literature suggests that each of the responses followed a polycentric approach, which seems a logical method for both of the cyber incident scenarios. Given the potential threat to the country and critical infrastructure, the contrast between the degree of response to each incident by both companies and the government appears inverted,

---

[189] Sanger, David E., Michael S. Schmidt and Nicole Perlroth. (December 14, 2014) Robertson, Jordan Robertson and Michael Riley. (February 19, 2015).
[190] Flowers, Angelyn, and Sherali Zeadally. (June 2014).
[191] Ashford, Warwick. (April 14, 2015): 4.

If the literature is correct, the risk to the economy and critical infrastructure is much higher in the JP Morgan Chase cyber incident because of its interconnectivity with critical financial infrastructure (DHS includes financial institutions as an element of U.S. critical infrastructure).[192] Further, the computer network exploitation on JP Morgan Chase is particularly concerning because a disruption to a major financial institution can have severe effects on the economic stability of the country and the world. In contrast, Sony is not considered part of the critical infrastructure nor was the attack on Sony assessed as one that would extend to other companies or other critical infrastructure.

The strong government response in the Sony case appears to manifest from the ability of the government to place attribution on a nation-state rather than a criminal organization. Despite the government's ability to attribute the acts and the initial condemnation, the follow through was lackluster, and, in some ways, further confused the government's policy for cyber incident response. The government first issued a threat to retaliate proportionally to the attacks, and then followed with a suggestion that the attacks conducted by North Korea were only a form of cyber vandalism.[193] This mixed reaction only causes confusion as many would ask how do you act

---

[192] Department of Homeland Security. (November 2013).
[193] Bradner, Eric. "Obama: North Korea's hack not war, but 'cybervandalism'." *CNN*. December 24, 2014. http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism/ (accessed March 3, 2015).

proportionally to cyber vandalism, and what does that mean about U.S. cyber policy?

It appears that despite contrasting views regarding the attribution of the Sony attack and the subsequent government response, the U.S. government does not have a way to fully assess the risk factors of cyberattacks.[194] Some of this is due to problems with attribution, but, despite this factor, the contrasting responses between these two cases show that there needs to be more work in developing models that help decision makers take appropriate actions.[195] These models must carefully consider the second and third order effects as well as alternative actor intent that may not be apparent on the surface. Regardless of the approach, future solutions need to address the current legal issues that hamper information sharing between the government and private industry.[196]

The government and the private sector have been wrestling with the legal implications of the private/government ownership and management of the Internet. Work to date, including the roadmap for collaborative action and the comprehensive cyber initiative; have yet to produce real methods for

---

[194] Berghel, H. (February 2015): 77-80.
[195] Ashford, Warwick. (April 14, 2015): 4.
Forsyth Jr., James Wood, and Maj Billy E. Pop. "Structural Causes and Cyber Effects: A Response to Our Critics." *Strategic Studies Quarterly* (International Security & Counter Terrorism Reference Center) 9, no. 2 (September 2015): 99-106.
[196] Fischer, Eric A., Edward C. Liu, John W. Rollins and Catherine A. Theohary. (December 2013).
Givens, Austen D., and Nathan E. Busch. "Integrating Federal Approaches to Post-Cyberattack Mitigation." *Journal Of Homeland Security & Emergency Management* (International Security & Counter Terrorism Reference Center) 10, no. 1 (April 2013): 1-28.

integrating risk assessment with polycentric response approaches vital to mitigating attacks in a hyperconnected world.[197]

[197] Chinn, David, James Kaplan, and Allen Weinberg. (January 2014).
Department of Defense. (July 2011).
Department of Defense. (November 2011).
Department of Defense. "DoD Cyber Strategy." *Defense.gov.* April 2015. http://www.defense.gov. (accessed May 5, 2015).
Executive Office of the President of the United States. "The Comprehensive National Cybersecurity Initiative." *http://www.whitehouse.gov/*. 05 2009. http://www.whitehouse.gov (accessed 09 15, 2013).

Chapter 3: Threat to Critical Infrastructure

Introduction

This chapter serves to explore the risk to United States critical infrastructure as defined by the Department of Homeland Security by cyber actors using Computer Network Attack (CNA) techniques on networked computer command and control and supporting systems.[198] Hypothesizing state actors such as China possess the capability to conduct crippling cyberattacks in U.S. critical infrastructure. The chapter will explore the risk by assessing malicious actor capabilities and intent, examining the vulnerability of the possible targets, the mitigations to those vulnerabilities currently in place, and the potential consequences of an attack.

Finally, this chapter will attempt to rationalize potential mitigation techniques for the assessed vulnerabilities. The chapter presents a literature review, assesses a case study concluding that cyberattacks on U.S. critical infrastructure are possible, wide scale full spectrum cyber warfare is unlikely, and the threat that state actors pose to the U.S. infrastructure is real, and requires further attention.

The cyber domain is unique in that it is the first man made warfighting domain, comprising a mix of hardware, software and people that continues to expand at an almost immeasurable pace. Like any other domain, man quickly began to look for ways to use this domain to improve its

[198] Department of Homeland Security. (November 15, 2013).

capability to wage warfare. First, integrating cyber technologies to communicate, detect enemy systems, and direct friendly systems and, eventually, developing ways to defend attack or exploit the adversary systems.

In the cyber domain, the enemy is transparent, attack can resemble defense, defense can resemble attack, and seemingly, benign activity can have grave effects. Attacks in the cyber domain often do not have a correlating effect in the physical world. This has implications for both the attacker and the defender. The attacker often cannot assess damage and defenders cannot easily assess whether the activity was an attack. Even if the defenders determine it was an attack, they often cannot determine who attacked.[199]

The outlined factors and others being discovered by researchers, make malicious activities that are effective in this microsecond potentially ineffective in the next. These challenges will continue to undermine the ability of any actor to wage war in the cyber domain at least in the near future. Despite the difficulty of waging full-scale cyber warfare, malicious cyber activities do pose a threat to national security, particularly in the area of economic security. These threats manifest through the theft of intellectual property and threats to critical infrastructure using network-connected systems as vulnerabilities. Despite the low probability of cyber warfare in the

[199] Singer, P.W., and Allan Friedman. Cybersecurity and Cyberwar, What Everyone Needs to Know. Oxford: Oxford University Press, 2014.

near term, the United States must prepare for the reality of the threat because potential adversaries are preparing themselves.

> *"The time for fundamental change in the battlefield – the arena of war – is not far off. Before very long, a network war or a nanometer war might become a reality in our midst, a type of war that nobody even imagined in the past. It is likely to be very intense, but with practically no bloodshed. Nevertheless it is likely to determine who is the victor and who is the vanquished in an overall war."* [200]

Literature Review

Because of the relative infancy of the cyber domain, there is limited work that specifically explores the consequences of a cyberattack to critical infrastructure as a mechanism for justifying war. In an attempt to conduct a complete analysis, the literature reviewed contains five main topics. These topics are technical threats, the threat actors and their intents as well as likely targets and their vulnerabilities. Examining cyberattack consequences and current policies rounds out the review.

Technical Threats

The literature available on the technical threat to critical infrastructure is quite vast. To narrow the scope, focus was placed on the most recent studies of the Chinese state-sponsored activities. Through examinations of the Mandiant report, which looked specifically at the vast capabilities the Chinese have with regard to computer network exploitation and a McAffee study that also looked at Chinese capabilities through a

[200] Liang, Qiao, and Wang Xiangsui. Unrestricted Warfare China's Master Plan to Destroy America. Panama: Pan American Publishing Company, 2002.

different approach, the various technical threats to critical infrastructure were assessed.[201] The latest reports on asymmetric attack vectors were also explored.

Threat Actors' Capabilities and Intent

The literature discussing threat actors is extensive. To narrow the study the literature review focused on the malicious Chinese cyber threat. The literature reviewed focuses on the categorization of threat actors. This provided insight on the degree of sophistication a threat actor must possess to conduct attacks on complex systems such as those found within critical infrastructure computer systems. One of the seminal documents was a Defense Science Board (DSB) study that helped to codify threat actors to narrow the focus.[202] The assessed threat actor was narrowed to the Chinese by examining Mandiant report congressional testimony and other resources such as the book *Unrestricted Warfare China's Master Plan to Destroy America.*[203] The China threat was chosen because it fell within a high threat Tier and their scope of detected and analyzed activities meets a threshold that could quickly manifest into physical, rather than virtual, consequences.

---

[201] Mandiant. (February 18, 2013).
McAfee. (December 29, 2010).
[202] Defense Science Board. (January 2013).
[203] United States Senate, One Hundred Sixth Congress. (2000).
Liang, Qiao, and Wang Xiangsui. (2002).
Mandiant. (February 18, 2013).
Office of the Secretary of Defense. Annual Report to Congress: Military and Security Developments Involving the People's Republic of China. Washington DC: Office of the Secretary of Defense, 2010.
ONCIX. "Foreign Spies Stealing US Economic Secrets in Cyberspace." *http://www.ncix.gov/*. October 2011. http://www.ncix.gov/ (accessed 09 15, 2013).

Threat Targets and Vulnerabilities

Possible targets and vulnerabilities were assessed through studies such as the congressional look into electrical grid vulnerabilities, and the North American Electric Reliability Corporation (NERC) Technical Analysis of the 2003 blackout.[204] The focus narrowed the threat to the electrical grid as the most likely target for attack.[205] Because of its antiquated structure, increasing number of remote operated computer controlled systems, and the intolerance the system has for minor disruptions, the electric grid contains the highest risk of substantial disruption.

Attack Consequences and Mitigations

To understand attack consequences, studies such as the Brookings paper on U.S. port and cyber vulnerabilities and congressional testimony were used to gather data regarding the assessed consequences of an attack on the electrical grid.[206] Other studies were also used to provide context for a nuclear power plant failure and the possibility of attacking computer controlled equipment in hardened facilities.[207] Current U.S. government

---

[204] NERC Steering Group. Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn? . Analysis, Princeton: NERC, 2004.
[205] Staff of Congressman Edward J. Markey. Electric Grid Vulnerability: Industry Response Reveal Security Gaps. Washington DC: U.S. House of Representatives, 2013.
U.S. Government Accountability Office. *Cybersecurity: Challenges in Securing the Electricity Grid.* Washington DC: U.S. Government Accountability Office, 2013.
[206] Kramek, Joseph. The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities. Paper, Washington, D.C.: Brookings, 2013.
Staff of Congressman Edward J. Markey. (2013).
U.S. Government Accountability Office. (2006).
U.S. Govt. Accountability Office. (2011).
U.S. Govt. Accountability Office. (2014).
[207] Kuschner, David. "The Real Story of Stuxnet How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program." *IEEE Spectrum*. February 26, 2013. spectrum.ieee.org/telecom/security/the-real-story-of-Stuxnet (accessed March 05, 2014).

strategies for cybersecurity were reviewed, as well as reports to Congress that provide context to the current mitigations in place and those that could be put into place.[208]

Current Policy on Cyberattacks

For a complete understanding of the policy implications cyberattacks have on critical infrastructure and the current posture of those, documents were reviewed from the National Security Strategy to the Department of Defense Strategy for Operating in Cyber Space and Department of Homeland Security strategy.[209] The policies of the U.S. government and its agencies were considered along with the needs and requirements of the private sector.[210] This was especially critical because currently the vast majority of networks, including those of the U.S. government, ride on private or corporate owned infrastructure.[211] The very nature of the networks poses an important set of challenges regarding the justification for implicating a malicious actor for committing an act of war and the subsequent justification for retaliation.

Riley, Michael. *U.S. Power Grid Vulnerable to Enemy Attack, Lawmakers Say*. May 23, 2013. http://www.bloomberg.com (accessed November 25, 2013).

[208] Anderson, Julie M, Karen S Evans, Franklin S Reeder, and Meghan M Wareham. "Measuring What Matters: Reducing Risk by Rethinking How We Evaluate Cybersecurity." *safegov.org*. 03 2013. http://www.safegov.org (accessed 10 21, 2013).

[209] Executive Office of the President of the United States. *National Security Strategy*. Washington DC: Office of the President of the United States, 2010.
Department of Defense. (July 2011).

[210] Asllani, Arben, Charles Stephen White, and Lawrence Ettkin. "Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals." *Journal Of Legal, Ethical & Regulatory Issues* (Business Source Complete) 16, no. 1 (January 2013): 7-14.
Baker, Stewart, Shaun Waterman, and George Ivanov. "In The Crossfire." *McAfee.com*. 2009. http://www.mcafee.com (accessed 09 15, 2013).

[211] Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. (April 2013): 1-27.

Threat Assessment Process

The Defense Science Board suggests a threat assessment model where risk is a function of the threat to a given target, the target's vulnerabilities and the consequences of a successful attack on the target.[212] The model itself is a standard representation that helps provide context to the terms used to describe the risk parameters such as threat, vulnerabilities, and consequences. Each of these terms has implications for both the friendly force and the opposition (see figure 1).

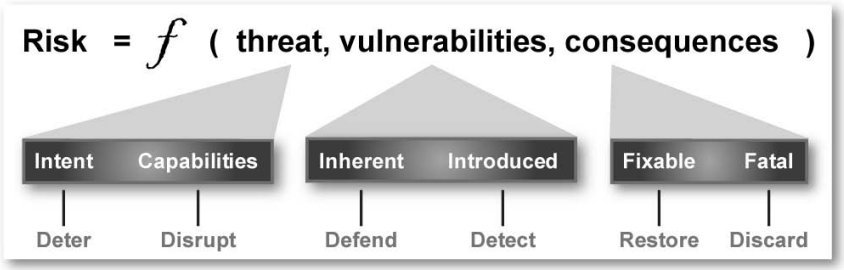

Figure 1: Risk Management Parameters [213]

By having a common frame, the risk can be assessed by weighing parameters such as the opposing forces' intent and capabilities against the friendly forces' ability to deter and disrupt the opposing force threat. This model was considered when organizing the discussion regarding the risk to targets within U.S. critical infrastructure from the threat of Cyberattacks.

[212] Defense Science Board. (January 2013): 6.
[213] Ibid: 6.

Malicious Cyber Activity Types

Assessing the threat to critical infrastructure requires understanding the types of activity cyber actors' conduct that may affect the systems that control and support the infrastructure. The popular media and even academia often misattribute some of these activities as cyberattacks. This misrepresentation could skew risk assessments to indicate an increased threat, thus exaggerating the likelihood of the consequences. It is particularly important to understand the types of activities that could be construed as attacks because the true Chinese threat is masked by the actual categorization of their activities as exploitation, intrusion and theft rather than the sensationalized use of computer network attack.

Some of the activities represented as Computer Network Attack (CNA) are more accurately Computer Network Exploitation (CNE). These activities represent several types of unauthorized and often illegal computer or network access. CNE can represent multiple activities such theft, hijacking, manipulation, or espionage.[214] Each of these activities, in most instances, does not cause physical destruction or disablement of the computer or system that is accessed, but, rather, the use of the system to gain a specific end the cyber actor intends without the expressed permission of the system owner.

[214] Department of Defense. "Joint Publication 3-12(R): Cyberspace Operations." *dtic.mil.* February 5, 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (accessed September 23, 2013).

In contrast to CNE, CNA is the deliberate destruction or disablement, either permanent or repairable, to a computer or network.[215] While CNE can be a threat to a company, country or person they are not intended to cause a physically manifested negative outcome like CNA. These outcomes can manifest themselves through network or system failures that cause critical infrastructure (such as power, water, transportation systems) to temporarily or permanently fail.[216] CNA is fundamentally different because the intent is to cause damage or disablement of a computer or network, an action that could be construed as an act of war.[217]

Table 1, below, describes some of the ways CNA is conducted to cause negative effects on networked systems. While not a complete list of threat sources, the table provides information on some of the more basic types and techniques used to conduct malicious activities on target networks. This is an important baseline of information because it represents some of the complexity that these 'attacks' provide that further obfuscate the origin of the attack.

[215] Department of Defense. (February 5, 2013).
[216] U.S. Government Accountability Office. (2006).
[217] Detter de Lupis Frankopan, Ingrid. *The Law of War. 3rd ed.* Farnham: Ashgate Publishing Ltd, 2013.

Table 1: Types and Techniques of Cyberattacks [218]

Threat Source	Description
Botnet	A network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for 'robots') are programs that are covertly installed on a targeted system allowing an unauthorized user to remotely control the compromised computer for a variety of malicious purposes.
Denial of Service	A method of attack that denies system access to legitimate users without actually having to compromise the targeted system. From a single source, the attack overwhelms the target computers with messages and blocks legitimate traffic. It can prevent one system from being able to exchange data with other systems or prevent the system from using the internet.
Distributed Denial of Service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit Tools	Publically available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic Bomb	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.
Malware	Malicious software designed to carry out annoying or harmful actions. Malware often masquerades as a useful program or is embedded into useful programs, so that users are induced into activating programs. Can also be installed without the user's knowledge to surreptitiously track or transmit data, or both to an unauthorized third party.

While CNA could be construed, as described above, as an act of war, most of the activities conducted thus far by the Chinese have fallen outside of the current description of acts of war and are better defined as illegal acts of theft. The following quote describes one opinion of when CNA would be an act of war.

> *"Planting a malicious virus in the computer network of an enemy can thus be highly effective to win advantage in military operations. This would be one method of cyberspace warfare. The intent with which such interference is carried out entitles it to be*

[218] Defense Science Board. (January 2013).

classified as an 'attack' in the sense of article 51 of the UN Charter which thus activates the right of self-defense." [219]

Threat Background

Malicious cyber activities target a wide variety of networked and stand-alone devices, ranging from individual electronic components to complex systems and systems of systems. While there is a multitude of vulnerable systems, the United States Critical Infrastructure is increasingly at risk due to the very advances in technology that improve its capability and capacity.[220] As critical infrastructures modernize, manual control processes are often upgraded to supervisory control and data acquisition systems (SCADA).[221] In the past, these industrial control systems (ICS) resided on internal networks and relied heavily on human controlled manual processes.[222] As these systems convert to SCADA, they integrated into networks to improve services and production while reducing the required human operators.[223] The increase of networked systems in critical infrastructure ICS such as production and distribution of water, power, sewer, oil, and natural gas have increased the ability for malicious actors to obtain access to SCADA systems.[224]

---

[219] Detter de Lupis Frankopan, Ingrid. (2013).
[220] Zhang, Zhen. "Cyberwarfare Implications for Critical Infrastructure Sectors." *The Homeland Security Review* 5, no. 3 (Fall 2001): 281-295.
[221] Malone, Eloise F., and Michael Malone. (August 2013): 158-177.
[222] Henrie, Morgan. "Cybersecurity Risk Management in the SCADA Critical Infrastructure Environment." *Engineering Management Journal* 25, no. 2 (June 2013): 38-45.
[223] Ibid: 38-45.
[224] Kesan, Jay P., and Carol M. Hayes. "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace." *Harvard Journal of Law & Technology* (Index to Legal Periodicals & Books Full Text (H.W. Wilson)) 25, no. 2 (Spring 2012): 415-529.

There are multiple possible threat actors: radical individuals, self-funded terrorist groups, and state funded cyberattack teams.[225] Each of these groups represents a possible threat to critical infrastructure; however, state-funded cyberattack teams represent the most critical threat.[226] State sponsored teams can use their capabilities to create vulnerabilities in the SCADA systems of critical infrastructure.[227] By creating vulnerabilities, state-sponsored threat actors can hold those systems at risk. Exploiting critical infrastructure can cause severe risk to a country's ability to conduct war, cause financial crisis, and in extreme instance loss of life.[228]

To understand the source of potential cyber threats the Defense Science Board broke them down into six categories outlining the description of the threat posed by each group. It is important to understand the difference each threat poses to assess the potential risk to critical infrastructure. The diversity of the group creates dilemmas for defining, deterring and responding to them.

Hactivists - Hacktivism refers to politically motivated attacks on publically accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into web sites to send a political message.[229]

---

[225] Defense Science Board. (January 2013).
[226] Ibid.
[227] Kesan, Jay P., and Carol M. Hayes. (Spring 2012): 444-445.
[228] Ibid: 444.
[229] Defense Science Board. (January 2013).

Hackers - Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.[230]

Criminal Groups - There is an increased use of cyber intrusions by criminal groups to attack systems for monetary gain.[231]

Insiders - Working from within an organization, the insider threat can be intentional or unintentional. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat remains one of the most significant cyber threats to the Department of Defense (DoD). The insider threat can also include contractor personnel.[232]

Terrorists - Terrorists seek to destroy, incapacitate, or exploit critical infrastructure to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. However,

[230] Defense Science Board. (January 2013).
[231] Ibid.
[232] Ibid.

traditional terrorist adversaries of the United States are less developed in their computer network capabilities state actors.[233]

Foreign Intelligence Services - Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. According to the Director of National Intelligence, "a growing array of state and non-state adversaries are increasingly targeting – for exploitation and potential disruption or destruction – information infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[234]

Threat actors create vulnerabilities by using unauthorized methods to intrude into computer systems. Once the cyber actors intrude into the system, they assess the system for vulnerabilities and either use previously developed malicious code or code and methods developed specifically for the victim system to damage, disrupt or destroy the software or hardware.

Mandiant's APT1 report recently brought to light one of the most aggressive state sponsored cyber threats an assertion that has been attested to by congressmen Rogers and Dutch in their Investigative Report on U.S. National Security Issues. *"China has the means, opportunity, and motive to use telecommunications companies for malicious purposes."*[235]

---

[233] Defense Science Board. (January 2013).
[234] Ibid.
[235] Mandiant. (February 2013).

APT1 analyzed massive intellectual property (IP) theft and implicated China in sponsoring the cyber actors conducting the activities.[236] While Mandiant's report focuses on China's cyber espionage unit and the sophistication of the tactics, techniques and procedures (TTP) China uses to exploit and pilfer U.S. companies, IP suggests they are an imminent threat to any networked system.[237] The important thing to note from this report is the characterization of the intrusions as attacks. Reports such as these, although a superb representation of an in depth investigation into Chinese cyber intrusions and theft, provide little or no justification for characterizing their activities as attacks.

The Defense Science Board suggests that state sponsored cyber teams have the most robust capabilities to exploit vulnerabilities and attack systems.[238] The DSB uses a six-tier system to categorize possible threats.[239] These threats have also been evaluated to assess the nominal investment required to develop the capabilities and are grouped in three levels; tier I-II from a few dollars to a few thousand dollars, III-IV in the millions, V-VI in the billions.[240]

Table 2, below, is representative of the Defense Science Board's tier breakout that categorizes practitioners by level of sophistication.

Rogers, Mike, and Ruppersberger Dutch. Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE. Congressional, Washington: U.S. House of Representatives, 2012.

[236] Mandiant. (February 2013).

[237] Ibid.

[238] Defense Science Board. (January 2013).

[239] Ibid.

[240] Ibid.

Table 2: Malicious Cyber Actor Tier Levels [241]

Tier I	Practitioners who rely on others to develop the malicious code, delivery mechanisms, and execution strategy (use known exploits)
Tier II	Practitioners with a greater depth of experience, with the ability to develop their own tools (from publically known vulnerabilities)
Tier III	Practitioners who focus on the discovery and use of unknown malicious code, are adept at installing user and kernel mode root kits, frequently use data mining tools, target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data with the expressed purpose of selling the information to other criminal elements
Tier IV	Criminal or state actors, who are organized, highly technical, proficient, well-funded professionals working in teams to discover new vulnerabilities and develop exploits
Tier V	State actors who create vulnerabilities through an active program to "influence" commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest
Tier VI	States with the ability to successfully execute full spectrum (cyber capabilities in combination with all of their military and intelligence capabilities) operations to achieve a specific outcome in political, military, economic, etc. domains and apply at scale

Using the DSB developed tier system and the information constructed in several reports such as Mandiant's APT1, the current known threat of the Chinese is in the level IV category. Tier IV status indicates that activity has been mostly expressed through cyber espionage and IP theft.[242] While there is no current evidence to support the argument that China has developed full spectrum capabilities, their current capacity suggests an aspiration toward that goal. One of the noted issues that the Mandiant report and others

[241] Defense Science Board. (January 2013).
[242] Defense Science Board. (January 2013).
Mandiant. (February 2013).

brought to light is the inherent difficulty in identifying the responsible threat actor beyond a reasonable doubt.[243] The anonymity of the Internet provides even state actors the ability to conduct vast operations with virtual impunity.

The recent report by Mandiant suggests that the APT1 cyber espionage unit examined consists of hundreds to thousands of individuals.[244] Provided this is only one of multiple possible units conducting cyber activities for China there is a strong possibility the full capacity of China to conduct cyberwar cannot be determined. However, the Mandiant report did provide the ability to hypothesize the possible damage China or other state sponsored actors could conduct given the assessed intrusions. Even a cursory assessment reveals that there have been compromises of industries that manage large portions of critical infrastructure including, transportation, navigation, satellites and telecommunication, and energy. Compromises, which if used to conduct an attack, could cause serious damage to national security.

Threat Actor Capabilities and Intent

Recent studies such as APT1, Operation Shady Rat, and the 2012 GAO study on economic espionage suggest that Chinese intentions focus on the theft of intellectual property.[245] The intent of the theft is interpreted in

---

[243] Mandiant. (February 2013).
[244] Ibid.
[245] Alperovitch, Dmitri. "Revealed: Operation Shady RAT." *www.mcafee.com*. August 02, 2011. http://www.mcafee.com (accessed 10 21, 2013).
U.S. Government Accountability Office. Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage. Washington DC: U.S. Government Accountability Office, 2012.

several ways. One suggestion might be that the theft is to gain military superiority by gaining advanced weaponry and assessing the vulnerabilities of U.S. weapons systems. A separate argument could be that by stealing data China can profit by reproducing products and edge the U.S. out of market share. A third argument might consider the theft espionage only if that information is being stolen to gain knowledge of U.S. intent.

While all of these arguments are plausible, the shortsightedness of thinking only one of these possibilities is the intent behind Chinese malicious activities is naïve at best. In *Unrestricted Warfare,* the authors suggest that China looks to destroy the United States through asymmetric attack.[246] While true intent can only be assessed by observation of acts, the capabilities the Chinese have developed for CNE provide them with a high degree of access that should there be intent they could easily shift their approach from theft and espionage to disruption and damage. The very development of the capability to exploit or intrude into systems can be said to have expressed the intent to hold those systems at risk of attack.

Targets within U.S. Critical Infrastructure

U.S. critical infrastructure consists of thousands of facilities, hundreds if not thousands of networks, both privately and publically owned, consisting of everything from water storage and treatment to nuclear power facilities.

Mandiant. (February 2013).

[246] Liang, Qiao, and Wang Xiangsui. (2002).

According to the Department of Homeland, defines "Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[247] The assets, systems, and networks that comprise the critical infrastructure are key targets to malicious state sponsored cyber actors. In most cases, these facilities are located in the U.S.; however, some facilities key to the U.S. are located in and even owned by other countries. By disrupting the services provided by these facilities, an opponent can cause varying degrees of harm from minor disruptions of service to full-scale shutdown of power, water or other critical services.

Target Vulnerabilities both Inherent and Introduced

There have been multiple assessments of various parts of U.S. critical infrastructure to determine the level of vulnerability. In one, Congress conducted a survey of over 100 utility companies, which concluded that the U.S. electrical grid is vulnerable to attack.[248] One of the findings noted that the companies surveyed reported their information systems either continuously probed for vulnerabilities or are routinely under attack by malicious actors.[249] General Alexander, Director of the National Security

[247] Department of Homeland Security. (November 15, 2013).
[248] Riley, Michael. (May 23, 2013).
[249] Ibid.

Agency, remarked that on a scale of one to 10 with 10 being the most prepared, U.S. critical infrastructure is only a three.[250]

Mandiant has perhaps best described the threat to critical infrastructure though its assessment of APT1. In the comprehensive but limited assessment, Mandiant identified 141 victims of compromise across a broad area of industry including some that contain networks in critical infrastructure.[251] Access these compromises afford can be used to conduct disruptive or destructive activities.

> *"The threat posed to U.S. national-security interests by vulnerabilities in the telecommunications supply chain is an increasing priority given: the country's reliance on interdependent critical infrastructure systems; the range of threats these systems face; the rise in cyber espionage; and the growing dependence all consumers have on a small group of equipment providers."*[252]

One of the key systems of systems in the U.S. critical infrastructure is the electrical grid. Because of the complexity of the system, small failures can have ripple effects proven to cause massive uncontrolled outages. In 2003, a rolling blackout occurred in the northeast United States and parts of Ontario, Canada due to a simple software glitch in an alarm system. As with many catastrophes, this very inconsequential glitch caused a failure that rippled

---

[250] Charles, Deborah. NSA chief says U.S. infrastructure highly vulnerable to cyberattack. 06 12, 2013. http://www.reuters.com (accessed 11 27, 2013).
[251] Mandiant. (February 2013).
[252] Rogers, Mike, and Ruppersberger Dutch. (2012).

outward, causing damage to other systems and eventually shutting down the power in some places for up to two days.[253]

Though the east coast outage was caused by imbalances in the network due to equipment failure, it provides a litmus test for how little would be required to cause serious outages, and even physical damage, to the grid. In a recent study, the Federal Energy Regulatory Commission suggested that a coordinated attack on as few as nine substations could cause a collapse of the entire electric grid for an undetermined amount of time.[254] While this study did not specifically look at cyberattack as a means for causing widespread destruction, it is an example of the limited number of disturbances in the system that might be required to cause such an effect.

To understand the vulnerability to the grid a complex cyberattack of this kind should be assessed to determine if the same results might be found. In any attack, military planners would assess that the simpler the approach, the more likely the attacker will execute the attack as planned, thus having a direct impact on the likelihood of success. This is based on a simple principle that proposes the more variables in any equation, the greater the risk of miscalculation.

---

[253] NERC Steering Group. (2004).
[254] Smith, Rebecca. "U.S. Risks National Blackout From Small-Scale Attack Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage." *Wall Street Journal*. March 12, 2014. http://online.wsj.com/news/articles/SB10001424052702304020104579433670284061220 (accessed 02 12, 2014).

Consequences of an Attack both Fixable and Fatal

In a recent paper that assessed the cyber threat to U.S. ports, the author suggested that an attack could cause serious consequences that could cause a ripple effect with far reaching consequences.[255]

> *"The potential consequences of even a minimal disruption of the flow of goods in U.S. ports would be high. The zero-inventory, just-in-time delivery system that sustains the flow of U.S. commerce would grind to a halt in a matter of days; shelves at grocery stores and gas tanks at service stations would run empty."*[256]

While an interruption is a serious concern, a deliberate attack could affect the safety features built into the power plants that provide the electricity for the grid. The recent Stuxnet worm that was indicated in targeted attacks on Iranian nuclear facilities provides insight into the capabilities a Tier V actor (see Table 2 for definition) can bring to bear on adversaries systems. Stuxnet was designed to specifically seek out, infect and damage the centrifuges Iran is using to enrich Uranium.[257] The skill and funding required to conduct the cyber exploit and the investment required to employ it could only have been doe by a state actor.

In a very similar instance a state actor such as China, using the vast capabilities they currently have to remotely access computer networks in the United States, could develop and target controls that manage power plants. One of the more disconcerting of these would be a targeted attack on the

[255] Kramek, Joseph. (2013).
[256] Ibid.
[257] Kuschner, David. (February 26, 2013).

safety controls of nuclear plants. While these plants have multiple redundancies, they are designed to work in a specific manner with very little flexibility. A clever team of state actors could feasibly find the weakness in the system and cause a meltdown.

Incidents such as Chernobyl and Three Mile Island provide analogous models proving the possibility of major incidents through minor failures. While in both of these incidents, there is a series of malfunctions and mistakes made by operators, a well-planned attack designed to provide false readings and manipulate computer controlled valves to replicate similar conditions could lead to a meltdown of unknown scale. These systems are continuously being upgraded to add remote operation capabilities; the vulnerabilities of these systems expand with each connection.

Even in a limited attack scenario where the system is ultimately fixable, a targeted attack that affects the U.S. military apparatus to conduct operations might be construed as an act of war. However, there are issues with characterizing a Chinese cyberattack scenario on the U.S. electrical grid as act of war. The primary issue is the difficulty of proving who conducted the attack. Only then would retaliatory actions be acceptable.

Current or Proposed Mitigation Techniques

Given the relative infancy of the cyber domain, the U.S. has very little capability to defend the critical infrastructure. One of the more prominent factors that complicate the ability to defend SCADA networks for critical

infrastructure is their private ownership.[258] The ability of the government to intrude into the privately owned networks of individuals and companies even for the purposes of defending them is outside current policy and acceptable behavior.

With the establishment of U.S. Cyber Command (CYBERCOM) in 2009, the Department of Defense began to consolidate its cyber capabilities. CYBERCOM's mission is to defend DoD networks and prepare to conduct full spectrum cyber operations. While CYBERCOM has worked diligently to develop and institute capabilities to defend DoD networks, the DoD does not have jurisdiction over most of the U.S. critical infrastructure, which leaves the privately owned portions more vulnerable to attack. To make matters more complicated, the Department of Homeland Security has the responsibility to find solutions to protect private networks and to collaborate with industry to meet that challenge. The encumbering misalignment of activities by the DoD and DHS causes further risk to critical infrastructure and alienates industry partners, ultimately decreasing cooperation.

One of the challenges for the U.S. government will be to implement policies that promote the security and redundancy of critical networks while respecting the privacy afforded under the Constitution. The unique nature of the problem will also require the government to work closely with allies and partners to develop international security agreements, terms of acceptable

[258] Kramek, J. (2013).
Luallen, Matthew E. SANS SCADA and Process Control Survey. SANS Analyst Program, 2013.

cyber activities, and, given the threat, an appropriate response to perceived cyberattack. The complexity of the Internet provides some mitigation through its continually growing and morphing structure.

To increase the cooperation of privately held companies the government will need to continue to build partnerships with private industry. These cooperative partnerships are required to develop, and implement standards that create methodologies to maintain privacy while sharing critical cybersecurity information. The government should begin by standardizing the reporting of cyberattacks across the USG by providing industry one process and one place to provide and receive incident information. The implementation of this process has been started but there is more work to be done in developing cross industry communication.

The government will also have to work more closely with the international community to develop acceptable standards of cyber conduct as well as develop legislation that provides funding or tax incentives to key industries that require heightened Cybersecurity measures to help manage implementation costs. This is particularly important for critical infrastructure owned by private industry.

The first priority for the government should be to work with the international community to set acceptable norms of activities in cyberspace. Setting norms is critical to creating an environment where all parties act and

react in a similar manner. Norms are also critical to avoid conflicts by providing common language to air grievances.

The current climate between policymakers and industry suggests there is recognition of the need for policy change particularly within the area of critical infrastructure and the Defense Industrial Base (DIB). Despite a loosely agreed upon cybersecurity reality, there persists a lack of trust between industry and government regarding security standardization, reporting procedures and cost allocations. Because of this lack of trust, any policy that affects industry will likely fail. Likewise, international agreements are difficult to ratify because of differing legal systems and cultural norms.

Despite the challenges presented by trust issues between industry and government and the complexities of developing international standards, there can be a managed way forward if government priorities change. The first change needed is for the government to conduct a full review of how industry interacts with each agency in partnership with those companies to determine best practices and align how the companies interact with government. The review should focus on changing what the government does to maximize its ability to assist industry and minimize cost to industry. This would include items such as streamlining incident reporting, decreasing required interactions with multiple agencies over the same incident or topic and

increasing the responsiveness and feedback industry receives for providing information to the government (return on investment).

Government should move simultaneously to develop evolving standards to secure its own unclassified networks and provide those free of charge to all U.S. industry. Further, government should identify methods to identify and categorize critical private networks and develop legislation to provide financial incentives for those companies to increase the security of the networks.

Finally, the government should continue to reach out to international institutions, both private and federally managed to build mutually acceptable agreements standardizing cyber norms. The proposed changes are in no way a comprehensive list but they do provide a stepping off point that the government can use to build a pathway of success for industry and the international community.

Conclusion

There is little doubt that in the complex and contested cyber domain there is a continued future for conducting malicious activities. The rate of expansion of networked connected devices used to manage critical infrastructure ensures continued exploitation. With this certainty comes the very real possibility that state sponsored cyber teams could reach a stage where full-scale cyberwar to disable, disrupt and even destroy U.S. critical infrastructure is possible.

> *"Preserving flexibility of U.S. response by maintaining some measure of ambiguity is useful, so long as we make parameters clear by laying down certain markers or selected redlines whose breach will not be tolerated."* [259]

While the future threat seems viable, the evidence suggests that wide scale full spectrum cyber warfare is not currently feasible and even minor attacks to critical infrastructure in many cases are unpalatable due to unpredictable ripple effects. Despite the unlikeliness of full-scale cyber warfare, the government and industry must work together to implement cybersecurity measures to protect critical infrastructure. Developing more robust security measures has mutual benefits for industry and government. Measures will help industry to protect its IP and maintain its viability in the global market and it will help government to insure common security for the nation's critical networks.

Regardless of the current possibility of a full scale cyberwar, the threat that China poses to the U.S. infrastructure through its repeated CNE and IP theft have reached a level that the U.S. government must consider whether China has already committed acts of war thought the degradation of the U.S. military advantage.[260] The asymmetric warfare approach of death by a thousand cuts may very well be underway. The implications of intrusions to the computer systems that support the military infrastructure such as satellites and communications, the energy sector, aerospace, and science and

---

[259] Cilluffo, Frank. "The U.S. Response to Cyber Threats." *Defense Dossier* (American Foreign Policy Council), 2012: 21-24.
[260] Schmitt, Michael. The Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press, 2013.

research, regardless of private ownership, need to be further scrutinized as the very ability for the U.S. to project power resides in the supporting infrastructure these industries provide. The U.S. must consider a new era where cyber domain plays a significant role in not only the prosecution of war but also in preparation for war.

Thesis Conclusion

The intent of this thesis was to explore malicious cyber threats through three different, but related areas: cybersecurity policy to prevent and deter attacks, the policy attempts to respond to malicious cyber activities with economic implications both during and after the attack and the risk associated with cyberattacks to critical infrastructure. The approach to this thesis was taken to analyze multiple dilemmas facing cybersecurity particularly as it applies to policy development, implementation and response. The overarching attempt was to expose the challenges the cybersecurity policy community has been struggling with since the inception of the Internet.

Chapter 1: Summary

Through analysis of two malicious cyber incidents, various cybersecurity policy approaches proposed in the literature are applied in an attempt to find reasonable governance processes for enhancing cybersecurity. These approaches were analyzed because it appeared that despite the extensive work done in response to cyber threats from multiple state and non-state actors, to date those policies have failed to provide adequate preventative cybersecurity. Further, the chapter seeks to assess if there is a cyber policy approach that provides preventative cybersecurity.

In a pure defense model the polycentric approach would likely be ideal because everyone with equity in the cyber domain commits to a security and

conduct framework willingly. The polycentric model, however, does not provide methods to thwart malicious cyber incidents. The state centric approach appears reasonable given the state is the normal body for defense of national assets; however, lack of jurisdiction limits implementation. Lastly, the active defense model is a conundrum in that active defense may in fact become offensive even though it implies a non-aggressive approach to implementing self-protection measures.

While there are more types of governance methodologies that could be explored, of the three main categories of governance processes for implementing preventative cybersecurity none of them stood out as the premier solution. In fact, it is likely that the best possible method is probably a hybrid of all of the solutions depending on the exact portion of the Internet being protected. This is not to suggest that any of these governance methodologies have the capability to prevent malicious cyber incidents. There was no evidence that any policy process would have the capability to deter or prevent cyber exploitation or attacks from a determined malicious actor.

Chapter 2: Summary

The second chapter in this series hypothesizes that current cyber incident response options are not adequate and fundamental changes to response approaches must be made. Using the governance processes from the first chapter, this chapter assesses whether or not they are adequate in a cyber incident response scenario. These approaches are chosen because to

remain consistent with the overall thesis and test the most common governance approaches in response scenarios.

The chapter tests this hypothesis through the examination two case studies one focused on a robust government response to a malicious cyber incident and a second where the government took a much less aggressive approach. These case studies were chosen to compare and contrast the government and private industry responses given the known and possible threat to the economy.

The response to the two cyber incidents were opposite of what should have been expected given the relative threat to the economy and in this case an identified part of U.S. critical infrastructure. Though the government did respond in both cases there appeared to be a failure to evaluate the responses as factors of risk to national security. In fact, the response to the Sony attack appeared to be emotionally driven instead of threat driven.

Chapter 3: Summary

The final chapter in the series used a standard threat assessment model to assess malicious cyber actor capabilities, and intent. The chapter uses this methodology to examine the vulnerability of select targets. The chapter then assesses mitigations to those vulnerabilities currently in place, and finally the potential consequences of a cyberattack.

The chapter uses a power failure, not caused by a cyberattack, as an analog of a cyberattack to the electrical grid. The electrical grid was chosen because it is identified as a part of U.S. critical infrastructure, the SCADA systems used to manage the network are increasingly connected to the Internet, and there are examples of SCADA manipulation for state actor exploitation.

Select mitigation techniques were evaluated for effectiveness and practicality of implementation. While not an all-encompassing assessment, the chapter concludes that there is a possibility that cyberattacks on U.S. critical infrastructure are possible current evidence suggests that wide scale full spectrum cyber warfare is unlikely. Further, because of the complexity of the SCADA systems even minor attacks to critical infrastructure in many cases is unpalatable to state actors because of unpredictable ripple effects that could cause unwanted escalation. Regardless of the current possibility of a full-scale cyberwar, the threat that state actors pose to the U.S. infrastructure is real and requires further attention.

Final Thoughts

Despite the relative infancy of the Internet, the response to cybersecurity, given the threat to critical infrastructure, the economy and private industry, is quite underwhelming. The depth of thought regarding cybersecurity including risk assessment, malicious cyber incident prevention, and response is quite extensive yet there seems to be no fundamental

breakthroughs in implementing any policies that properly assess cyber risk in a timely fashion, provide adequate defense or even response models.

Part of the difficulty in making strides in cybersecurity is the lack of congressional action. The Cybersecurity Information Sharing Act or CISA has been through two congresses without resolution. Some may assume that lack of congressional organization is what is stalling cyber policy however the complexity of regulating the Internet is likely the reason that policy has not progressed. There are far to many risks in violating both individual rights of Internet users and violating sovereign rights of other countries when deciding to implement regulations that will affect a system that is globally interconnected.

The resolution of the sovereign control versus multi-stakeholder or polycentric governance models is one that will ultimately be played out over numerous rounds of negotiation. In the end there will be some countries that move more toward a sovereign control model and some that will attempt to implement a global governance model. There are pitfalls in either but in order to maintain the global system a polycentric model is the only one that provides enough deterrent to malicious actors because in a cooperative polycentric model the odds of prosecution increase and reduce the safe-havens bad actors currently take advantage of.

The issue of active defense being used also complicates a system where there are sovereignty issues. The global nature of the Internet and the

entities that use it, such as international corporations, complicates any state run active defense system where the state uses sovereign rights in a system that is inherently difficult to draw sovereign boundaries. If the governance went to a polycentric model the active defense rights of each member could pre-coordinated, however implementing active defense would still be a monumental challenge that involves extensive carful negotiation to avoid inadvertent damage and even escalation.

Organization of cyber defense is also muddled with various stakeholders and action arms from the National Security Agency to the Department of Homeland Security and the Federal Bureau of Investigation to the Defense Department and Cyber Command not to mention the private firms who sell services to protect networks. While the resources are being allocated the organization and implementation does not appear aligned to drive the organizations into a successful model. In order to create a cyber defense model that works there should be changes made in the organization of the response force.

One of the first changes that should be made is the division of the National Security Agency and CYBERCOM. This is a fundamentally flawed marriage that has two entities that have competing equities being run by the same leader. These types of organizations rarely work and in the business world are broken up to increase competition ultimately making both organizations healthier.

In contrast the activities of the Department of Homeland Security and the Federal Bureau of Investigation seem to be aligned well. While the FBI cyber defense and response teams could always use more funding, adding additional funds without addressing the organizational alignment issues with the whole of government will not resolve the overarching issue of resource allocation and capability alignment.

One of the fundamental issues with the current governance processes is the failure to use existing risk assessment models. The contrast between the government response between the Sony and JP Morgan Chase case studies is a prime example of the imbalanced application of a risk assessment. Further, risk assessment model implementation needs to be more agile in assessing possible second and third order effects. This failure is apparent in the JP Morgan Chase case that where the government removed its state actor experts from the response team despite the risk to the economy had JP Morgan Chase been unable to rebuff the malicious actors.

Another important issue future policy solutions must tackle is the current legal hurdles that hamper information sharing between the government and private industry. Ultimately, however, the most challenging problem is the structure of the current Internet. In order to secure the Internet there may need to be a fundamental change its base structure. While not a solution that seems cost effective, or in many ways even possible,

an alternate Internet designed from the ground up for security is a possible solution.

One of the topics explored that warrant further research is the legal methodology for sharing threat information between the government and private industry. This one factor alone will suffice to provide countless doctoral papers, as the complexity of sharing information in the complex legal environment will continue to be a challenge. Secondly, the development a methodology for policymakers to make swift risk assessments with possible second and third order effects during cyber incidents would compliment current work already available and help drive appropriate reactions to future events. Finally, further work could be done in the area of cyber incidents in context of proportionality to determine what if any proactive (pre-attack) or reactive actions might be acceptable.

Bibliography

Albanesius, Chloe. "Why 2015 May Be the Year We Solve Net Neutrality." *PC Magazine*, February 01, 2015: 12.

Alperovitch, Dmitri. "Revealed: Operation Shady RAT." *www.mcafee.com*. August 02, 2011. http://www.mcafee.com (accessed 10 21, 2013).

Anderson, Julie M, Karen S Evans, Franklin S Reeder, and Meghan M Wareham. "Measuring What Matters: Reducing Risk by Rethinking How We Evaluate Cybersecurity." *safegov.org*. 03 2013. http://www.safegov.org (accessed 10 21, 2013).

Ando, Ritsuko. "Sony CEO sees no major financial impact from cyber Attack." *Reuters*. January 6, 2015. http://uk.reuters.com/article/2015/01/06/uk-sony-cybersecurity-idUKKBN0KF1ZH20150106 (accessed June 21, 2015).

Ashford, Warwick. "Problems in attributing cyber attacks could foil US sanctions against hackers." *Computer Weekly*, April 14, 2015: 4.

Asllani, Arben, Charles Stephen White, and Lawrence Ettkin. "Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals." *Journal Of Legal, Ethical & Regulatory Issues* (Business Source Complete) 16, no. 1 (January 2013): 7-14.

Baker, Stewart, Shaun Waterman, and George Ivanov. "In The Crossfire." *McAfee.com*. 2009. http://www.mcafee.com (accessed 09 15, 2013).

Bauer, Johannes M., and Michel Van Eeten. "Introduction to the Economics of Cybersecurity." *Communications and Strategies*, no. 81 (1st Quarter 2011): 13-21.

BBC. "Sony cyber-attack: North Korea faces new US sanctions." *BBC*. January 3, 2015. http://www.bbc.com/news/world-us-canada-30661973 (accessed April 5, 2015).

Berghel, H. "Cyber Chutzpah: The Sony Hack and the Celebration of Hyperbole." *Computer* 48, no. 2 (February 2015): 77-80.

Bonner, Lance. "Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches." *Washington University Journal of Law & Policy*, no. 40 (November 2012): 257-277.

Bradner, Eric. "Obama: North Korea's hack not war, but 'cybervandalism'." *CNN*. December 24, 2014. http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism/ (accessed March 3, 2015).

Brechbuhl, Hans, et al. "Protecting Critical Information Infrastructure: Developing Cybersecurity Policy." *Information Technology For Development* (Business Source Complete) 16, no. 1 (January 2010): 83-91.

Broggi, Jeremy J. "Building on Executive Order 13,636 to Encourage Information Sharing for Cybersecurity Purposes." *Harvard Journal Of Law & Public Policy* (Business Source Complete) 37, no. 2 (2014): 653-676.

Brunnstrom, David and Jim Finkle. "U.S. considers 'proportional' response to Sony hacking attack." *Reuters*. December 18, 2014. http://www.reuters.com/article/2014/12/19/us-sony-cybersecurity-northkorea-idUSKBN0JW24Z20141219 (accessed March 2, 2015).

Business Week. "Why the Target Data Hack Is Just the Beginning." *Business Week* (Business Week), no. 4363 (January 2014): 8.

Cashell, Brian, William D. Jackson, Mark Jickling, and Baird Webel. *The Economic Impact of Cyber-Attacks*. Report, Government and Finance Division, Congressional Research Service, Washington, D.C.: Congressional Research Service, 2004.

CBS News. *Files of more than 40,000 federal workers breached in cyberattack*. December 18, 2014. http://www.cbsnews.com/news/files-of-more-than-40000-federal-workers-breached-in-cyberattack/ (accessed March 25, 2015).

Center for Strategic and International Studies. "Net Losses: Estimating the Global Cost of Cybercrime." *Center for Strategic and International Studies*. June 2014. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf (accessed May 9, 2015).

—. "Significant Cyber Incidents Since 2006." *Center for Strategic and International Studies*. March 10, 2014. http://csis.org/files/publication/140310_Significant_Cyber_Incidents_Since_2006.pdf (accessed June 1, 2105).

—. "The Economic Impact of Cybercrime and Cyber Espionage." *Center for Strategic and International Studies*. July 2013. http://csis.org/publication/economic-impact-cybercrime-and-cyber-espionage (accessed March 2, 2015).

Charles, Deborah. *NSA chief says U.S. infrastructure highly vulnerable to cyber attack*. 06 12, 2013. http://www.reuters.com (accessed 11 27, 2013).

Chinn, David, James Kaplan, and Allen Weinberg. "Risk and responsibility in a hyperconnected world." *McKinsey.com*. January 2014. http://www.mckinsey.com/~/media/mckinsey/dotcom/insights/business

%20technology/risk%20and%20responsibility%20in%20a%20hyperconnected%20world%20implications%20for%20enterprises/risk%20and%20responsibility%20in%20a%20hyperconnected%20world.ashx (accessed March 2, 2015).

Cilluffo, Frank. "The U.S. Response to Cyber Threats." *Defense Dossier* (American Foreign Policy Council), 2012: 21-24.

Clark, Meagan. "Timeline of Target's Data Breach And Aftermath: How Cybertheft Snowballed For The Giant Retailer." *International Business Times*. May 5, 2014. http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056 (accessed April 2, 2015).

Coldebella, Gus P., and Brian M. White. "Foundational Questions Regarding the Federal Role in Cybersecurity." *Journal Of National Security Law & Policy* (International Security & Counter Terrorism Reference Center) 4, no. 1 (January 2010): 233-245.

Contreras, Jorge L., Laura Denardis, and Melanie Teplinsky. "Mapping Today's Cybersecurity Landscape." *American University Law Review* (Index to Legal Periodicals & Books) 62, no. 5 (June 2013): 1113-1130.

Defense Science Board. "Resilient Military Systems and the Advanced Cyber Threat." *Defense Science Board*. January 2013. http://www.acq.osd.mil (accessed 09 15, 2013).

DeNardis, L. "E-Governance Policies for Interoperability and Open Standards." *Policy & Internet* 2 (2010): 129–164.

Department of Defense. "Defense.gov." *Department of Defense Strategy for Operating in Cyberspace*. July 2011. http://www.defense.gov (accessed September 25, 2013).

—. "Department of Defense Cyberspace Policy Report." *www.defense.gov*. November 2011. www.defense.gov (accessed 09 15, 2013).

—. "DoD Cyber Strategy." *Defense.gov*. April 2015. http://www.defense.gov. (accessed May 5, 2015).

—. "Joint Publication 3-12(R): Cyberspace Operations." *dtic.mil*. February 5, 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (accessed September 23, 2013).

Department of Homeland Security. *dhs.gov*. 11 15, 2013. http://www.dhs.gov/what-critical-infrastructure (accessed 11 15, 2013).

Detter de Lupis Frankopan, Ingrid. *The Law of War. 3rd ed.* Farnham: Ashgate Publishing Ltd, 2013.

Devlin, Barrett and Danny Yadron. "Sony, U.S. Agencies Fumbled After Cyberattack; Lack of Information and Consultation Led to Flip-Flops,

Confusion." *The Wall Street Journal.* February 22, 2015. http://search.proquest.com/docview/1657238447?accountid=11752. (accessed March 2, 2015).

Elgan, Mike. "Why the Sony Hack Is the Start of Endless Cyber-War." *Eweek*, December 29, 2014: 1.

Ellis, Ralph, Holly Yan and Kyung Lah. "U.S. seeks China's help against North Korean cyberattacks." *CNN.* Decenber 20, 2014. http://www.cnn.com/2014/12/20/world/asia/north-korea-sony-response/ (accessed March 2, 2015).

Executive Office of the President of the United States. "International Strategy for Cyberspace." *www.whitehouse.gov.* May 2011. www.whitehouse.gov (accessed 09 15, 2013).

Executive Office of the President of the United States. *National Security Strategy.* Washington DC: Office of the President of the United States, 2010.

—. "Statement by the Press Secretary on the Executive Order Entitled “Imposing Additional Sanctions with Respect to North Korea”." *Whitehouse.gov.* January 2, 2015. https://www.whitehouse.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s (accessed March 2, 2015).

—. "The Comprehensive National Cybersecurity Initiative." *http://www.whitehouse.gov/.* 05 2009. http://www.whitehouse.gov (accessed 09 15, 2013).

Farwell, James P. "Industry's Vital Role in National Cyber Security." *Strategic Studies Quarterly* (International Security & Counter Terrorism Reference Center) 6, no. 4 (Winter 2012): 10-41.

Ferraro, Matthew F. "Groundbreaking" or broken? An analysis of SEC Cybersecurity disclosure guidance, its effectiveness, and implications." *Albany Law Review* (Academic Search CompleteEBSCOhost (accessed June 28, 2015).) 77, no. 2 (April 2014): 297-347.

Fischer, Eric A., Edward C. Liu, John W. Rollins, and Catherine A. Theohary. *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress.* Report, Congressional Research Service, Washington, D.C.: International Security & Counter Terrorism Reference Center, December.

Flowers, Angelyn, and Sherali Zeadally. "US Policy on Active Cyber Defense." *Journal Of Homeland Security & Emergency Management* (International Security & Counter Terrorism Reference Center) 11, no. 2 (June 2014).

Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. "Cybersecurity and US Legislative Efforts to address Cybercrime." *Journal Of Homeland Security & Emergency Management* (International Security & Counter Terrorism Reference Center) 10, no. 1 (April 2013): 1-27.

Forsyth Jr., James Wood, and Maj Billy E. Pop. "Structural Causes and Cyber Effects: A Response to Our Critics." *Strategic Studies Quarterly* (International Security & Counter Terrorism Reference Center) 9, no. 2 (September 2015): 99-106.

Fox News. *Hacker attack on federal security contractor not noticed for months, report claims.* November 4, 2014. http://www.foxnews.com/tech/2014/11/04/hacker-attack-on-federal-security-contractor-not-noticed-for-months-report/ (accessed March 28, 2015).

Givens, Austen D., and Nathan E. Busch. "Integrating Federal Approaches to Post-Cyber Incident Mitigation." *Journal Of Homeland Security & Emergency Management* (International Security & Counter Terrorism Reference Center) 10, no. 1 (April 2013): 1-28.

Glazer, Emily. *J.P. Morgan's Cyber Attack: How The Bank Responded* . October 3, 2014. http://blogs.wsj.com/moneybeat/2014/10/03/j-p-morgans-cyber-attack-how-the-bank-responded/ (accessed April 5, 2015).

Glenny, Misha, and Camino Kavanagh. "800 Titles but No Policy—Thoughts on Cyber Warfare." *American Foreign Policy Interests* (Academic Search Complete) 34, no. 6 (November 2012): 287-294.

Goldstein, Matthew, Nicole Perlroth, and David E. Sanger. *Hackers' Attack Cracked 10 Financial Firms in Major Assault.* October 3, 2014. http://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-assault/?_r=0 (accessed April 4, 2015).

Grant, Gerry H., and C. Terry Grant. "SEC Cybersecurity Disclosure Guidance is Quickly Becoming a Requirement." *CPA Journal* (Business Source Complete) 84, no. 5 (June 2014): 69-71.

Greenberg, Andy. *McAfee Explains The Dubious Math Behind Its 'Unscientific' $1 Trillion Data Loss Claim.* August 03, 2012. http://www.forbes.com (accessed 10 21, 2013).

Greenwald, Eric A. "History Repeats Itself: The 60-Day Cyberspace Policy Review in Context." *Journal Of National Security Law & Policy* (International Security & Counter Terrorism Reference Center) 4, no. 1 (January 2010): 41-62.

Haggard, Stephan, and Jon R. Lindsay. "North Korea and the Sony Hack: Exporting Instability Through Cyberspace." *Asiapacific Issues*, no. 117 (May 2015): 1-8.

Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. "Leaving Deterrence Behind: War-Fighting and National Cybersecurity." *Journal Of Homeland Security & Emergency Management* (International Security & Counter Terrorism Reference Center) 7, no. 1 (January 2010): 1-24.

Heilbrun, Mark R., and Isaac Brown. "Cybersecurity Policy and Legislation in the 112th Congress." *Intellectual Property & Technology Law Journal* (Business Source Complete) 23, no. 12 (December 2011): 14-20.

Henrie, Morgan. "Cyber Security Risk Management in the SCADA Critical Infrastructure Environment." *Engineering Management Journal* 25, no. 2 (June 2013): 38-45.

Hunker, Jeffrey. "U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away." *Journal Of National Security Law & Policy* (International Security & Counter Terrorism Reference Center) 4, no. 1 (2010): 197-216.

Ingersoll, Geoffrey. "US NAVY: Hackers 'Jumping The Air Gap' Would 'Disrupt The World Balance Of Power'." *Chron.com*. 11 19, 2013. http://www.chron.com (accessed 11 19, 2013).

Inserra, Paul Rosenzweig and David. *Government Cyber Failures Reveal Weaknesses of Regulatory Approach to Cybersecurity*. June 13, 2013. http://www.heritage.org/research/reports/2013/06/weaknesses-of-a-regulatory-approach-to-cybersecurity (accessed April 3, 2015).

International Institute of Communications. *International Institute of Communications*. April 6, 2015. http://www.iicom.org/ (accessed April 6, 2015).

Jayakumar, Amrita. *USIS cuts more than 2,500 jobs after losing contracts in wake of cyberattack*. October 7, 2014. http://www.washingtonpost.com/business/capitalbusiness/usis-cuts-more-than-2500-jobs-after-losing-contracts-in-wake-of-cyberattack/2014/10/07/5816cfb2-4e3f-11e4-babe-e91da079cb8a_story.html (accessed April 2, 2015).

Jensen, Eric Talbot. "Cyber Deterrence." *Emory International Law Review* (Index to Legal Periodicals & Books Full Text (H.W. Wilson)) 26, no. 2 (October 2012): 773-824.

Kahn, Robert E, et al. *America's Cyber Future: Security and Prosperity in the Information Age.* Washington DC: Center for a New American Security, 2011.

Kedmey, Dan. "Time.com." *Shoppers Just Don't Care About Credit Card Hacks.* November 20, 2014. http://time.com/3595186/target-home-depot-credit-card-hacks/ (accessed April 2, 2015).

Kesan, Jay P., and Carol M. Hayes. "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace." *Harvard Journal of Law & Technology* (Index to Legal Periodicals & Books Full Text (H.W. Wilson)) 25, no. 2 (Spring 2012): 415-529.

Klimburg, Alexander. *National Cyber Security Framework Manual.* NATO CCD COE Publications, 2012.

Kramek, Joseph. *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities.* Paper, Washington, D.C.: Brookings , 2013.

Krebs, Brian. *Target Hackers Broke in Via HVAC Company.* February 5, 2014. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ (accessed April 2, 2015).

Kueter, Jeff. "Cybersecurity: Challenging Questions with Incomplete Answers." *High Frontier,* , August 2010: 28-30.

Kuschner, David. "The Real Story of Stuxnet How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program." *IEEE Spectrum.* 02 26, 2013. spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (accessed 03 05, 2014).

Laughland, Oliver and Dominic Rushe. "Sony cyber attack linked to North Korean government hackers, FBI says." *The Guardian.* December 19, 2014. http://www.theguardian.com/us-news/2014/dec/19/north-korea-responsible-sony-hack-us-official (accessed March 2, 2015).

Lawson, Sean. "Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States." *First Monday*, 2012.

Lemos, Robert. "Sony Pegs Initial Cyber-Attack Losses at $35 Million." *Eweek.com.* February 4, 2015. http://www.eweek.com/security/sony-pegs-initial-cyber-attack-losses-at-35-million.html (accessed March 12, 2015).

Lewis, Ted G., and Rudy Darken. "Potholes and Detours in the Road to Critical Infrastructure Protection Policy." *Homeland Security Affairs* (NPS Center for Homeland Defense and Security) 1, no. 1 (August 2005): 177.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare China's Master Plan to Destroy America.* Panama: Pan American Publishing Company, 2002.

Logiurato, Brett. "REPORT: 'Russians' Behind Huge JPMorgan Cyberattack." *Business Insider.* October 4, 2014. http://www.businessinsider.com/jpmorgan-cyber-attack-russian-breach-sanctions-2014-10 (accessed March 2, 2015).

Luallen, Matthew E. *SANS SCADA and Process Control Survey.* SANS Analyst Program, 2013.

Malone, Eloise F., and Michael Malone. "The "wicked problem" of cybersecurity policy: analysis of United States and Canadian policy response." *Canadian Foreign Policy Journal* 19, no. 2 (August 2013): 158-177.

Mamiit, Aaron. "Sony Pictures Cyber Attack May Cost $100 Million, Says Expert." *Tech Times.* December 10, 2014. http://www.techtimes.com/articles/21869/20141210/sony-pictures-cyber-attack-may-cost-100-million-says-expert.htm (accessed March 2, 2015).

Mandiant. "APT1: Exposing One of China's Cyber Espionage Units." *Mandiant Intelligence Center Report.* February 18, 2013. http://intelreport.mandiant.com (accessed 09 25, 2013).

Marketwatch. *JPMorgan Chase & Co.* April 7, 2015. http://www.marketwatch.com/investing/stock/jpm (accessed April 7, 2015).

McAfee. "A Good Decade for Cybercrime." *www.mcafee.com.* 12 29, 2010. http://www.mcafee.com (accessed 10 21, 2013).

McCracken, Harry. *How Target Made Itself a Target for Hackers.* March 15, 2014. http://time.com/23786/target-data-breach/ (accessed April 2, 2015).

Medici, Andy. *DHS, OPM suspend contracts with USIS after major cyber attack.* August 7, 2014. http://archive.federaltimes.com/article/20140807/IT/308070009/DHS-OPM-suspend-contracts-USIS-after-major-cyber-attack (accessed March 25, 2015).

Melnik, Tatiana. "New U.S. Sanctions Program Seeks to Give Government an Extra Tool to Fight Cyber-Attacks." *Journal of Health Care Compliance* (Business Source Complete) 17, no. 3 (May 2015): 53-56.

Munoz, Eduardo. *JPMorgan hack exposed data of 83 million, among biggest breaches in history.* October 2, 2014.

www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003 (accessed April 5, 2015).

Nakashima, Ellen. "Why the Sony hack drew an unprecedented U.S. response against North Korea." *The Washington Post*. January 2015. http://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html (accessed April 23, 2015).

NERC Steering Group. *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?* . Analysis, Princeton: NERC, 2004.

Newmeyer, Kevin P. "Who Should Lead U.S. Cybersecurity Efforts?" *PRISM Security Studies Journal* (International Security & Counter Terrorism Reference Center) 3, no. 2 (March 2012): 115-126.

Office of the Secretary of Defense. *Annual Report to Congress: Military and Security Developments Involvin the People's Republic of China.* Washington DC: Office of the Secretary of Defense, 2010.

ONCIX. "Foreign Spies Stealing US Economic Secrets in Cyberspace." *http://www.ncix.gov/*. October 2011. http://www.ncix.gov/ (accessed 09 15, 2013).

Opderbeck, David W. "Cybersecurity and Executive Power." *Washington University Law Review* (Index to Legal Periodicals & Books) 89, no. 4 (May 2012): 795-845.

Opderbeck, David W. "Does the Communications Act of 1934 Contain a Hidden Internet Kill Switch? ." *Journal Federal communications law journal* 65, no. 1 (January 2013): 1-46.

Organisation for the prohibition of chemical weapons. "Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction." *Organisation for the prohibition of chemical weapons.* July 29, 2005. https://www.opcw.org/index.php?eID=dam_frontend_push&docID=6357 (accessed April 7, 2015).

Oxford Economic. "Cyber-attacks: Effects on UK Companies." *Oxford Economic.* July 2014. http://www.cpni.gov.uk/documents/publications/2014/oxford-economics-cyber-effects-uk-companies.pdf?epslanguage=en-gb (accessed May 9, 2015).

Paganini, Pierluigi. *The network of USIS compromised by a cyber attack* . August 12, 2014. http://securityaffairs.co/wordpress/27499/cyber-

crime/network-usis-compromised-cyber-attack.html (accessed April 1, 2015).

Pellerin, Cheryl. *Defense.gov.* Edited by American Forces Press Service. July 01, 2013. http://www.defense.gov (accessed 10 21, 2013).

Ponemon Institute. "2014 Cost of Cyber Crime Study: United States." *Ponemon Institute.* October 2014. http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf (accessed March 2, 2015).

—. "2014 Global Report on the Cost of Cyber Crime." *Ponemon Institute.* October 2014. http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/ (accessed June 5, 2015).

Reyes, Anthony. "The Financial Crisis Five Years Later: Response, Reform, and Progress in Charts." *U.S. Treasury.* September 2013. http://www.treasury.gov/connect/blog/Documents/FinancialCrisis5Yr_vFINAL.pdf (accessed June 7, 2015).

Riley, Michael. *U.S. Power Grid Vulnerable to Enemy Attack, Lawmakers Say.* May 23, 2013. http://www.bloomberg.com (accessed November 25, 2013).

Riley, Michael, et al. "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It." *Bloomberg.com.* March 13, 2014. http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data (accessed April 2, 2015).

Risk Based Security. *A Breakdown and Analysis of the December, 2014 Sony Hack.* December 5, 2014. www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/ (accessed June 4, 2015).

Roberts, Paul F. and Paul Kielstra. "Measuring the cost of cybercrime." *The Economist.* Edited by Riva Richmond. May 20, 2013. http://www.economistinsights.com/technology-innovation/analysis/measuring-cost-cybercrime (accessed June 5, 2015).

Robertson, Jordan Robertson and Michael Riley. "JPMorgan Goes to War." *Bloomberg BusinessWeek.* February 19, 2015. http://www.bloomberg.com/news/articles/2015-02-19/jpmorgan-hires-cyberwarriors-to-repel-data-thieves-foreign-powers (accessed March 2, 2015).

Rogers, Mike, and Ruppersberger Dutch. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE.* Congressional, Washington: U.S. House of Representatives, 2012.

Rogers, Mike, Michael Hayden, and Paul Stockton, interview by Ellen Nakashima. *Lights, Camera… Hack! Strategic Implications of the Sony Cyber Attack*Edited by Blaise Misztal. Bipartisan Policy Center, (January 15, 2015).

Rogin, Josh. *The Cable*. July 9, 2012. http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history (accessed 10 19, 2013).

Roman, Jeffrey. "JPMorgan Confirms Cyber-Attack." *Bank Info Security*. September 15, 2014. http://www.bankinfosecurity.com/jpmorgan-a-7319 (accessed March 2, 2015).

Rushe, Dominic. "JP Morgan Chase reveals massive data breach affecting 76m households." *The Guardian*. October 3, 2014. http://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach (accessed April 5, 2015).

Sanger, David E., Michael S. Schmidt and Nicole Perlroth. "Obama Vows a Response to Cyberattack on Sony." *The New York Times*. December 14, 2014. http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html (accessed March 12, 2015).

Schmidt, Howard, interview by Cameron and Mustafa Safdar Parsons. *Defending Cyberspace: The View from Washington* (April 11, 2011).

Schmitt, Michael. *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press , 2013.

Schwitz, John G. "Risk-Based Cybersecurity Policy." *American Intelligence Journal* (International Security & Counter Terrorism Reference Center) 29, no. 1 (March 2011): 115-125.

Sha, Sooraj. "Will Sony really see no financial impact from cyber-attack?" *Computing*. January 8, 2015. http://www.computing.co.uk/ctg/news/2389309/will-sony-really-see-no-financial-impact-from-cyber-attack (accessed June 2, 2015).

Shackelford, Scott J, and Amanda N Craig. "Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity." *Stanford Journal Of International Law* (Academic Search Complete) 50, no. 1 (2014): 119-184.

Shackelford, Scott J. "Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance." *American University Law Review* (OmniFile) 62, no. 5 (June 2013): 1273-1364.

Shaw, C. Mitchell. "FBI Wrong on Sony Hack." *New American* 31, no. 4 (February 2015): 22-25.

Sicard, Sarah. "North Korean Cyber Attack on Sony Poses Tough Security Questions." *National Defense* 99, no. 736 (March 2015): 24-25.

Silver-Greenberg, Jessica and Matthew Goldstein. "After Breach, Push to Close Security Gaps." *The New York Times.* October 22, 2014. (accessed March 2, 2015).

Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar, What Everyone Needs to Know.* Oxford: Oxford University Press, 2014.

Singh, J. P. "Multilateral Approaches to Deliberating Internet Governance." *Policy & Internet* 1 (2009): 91-111.

Smith, Rebecca. "U.S. Risks National Blackout From Small-Scale Attack Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage." *Wall Street Journal.* 03 12, 2014. http://online.wsj.com/news/articles/SB10001424052702304020104579433670284061220 (accessed 02 12, 2014).

Staff of Congressman Edward J. Markey. *Electric Grid Vulnerability: Industry Respones Reveal Security Gaps.* Washington DC: U.S. House of Representatives, 2013.

Taylor, Brian. "Cyber attacks fallout could cost the global economy $3 trillion by 2020." *Tech Republic.* February 20, 2014. http://www.techrepublic.com/article/cyberattacks-fallout-could-cost-the-global-economy-3-trillion-by-2020/ (accessed March 2, 2015).

U.S. Government Accountability Office. *Cybersecurity: Challenges in Securing the Electricity Grid.* Washington DC: U.S. Government Accountability Office, 2013.

U.S. Government Accountability Office. *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented.* Washington DC: U.S. Government Accountability Office, 2013.

—. "DOD Faces Challenges In Its Cyber Activities." *Defense Department Cyber Effort.* July 25, 2011. http://www.gao.gov (accessed 09 25, 2013).

U.S. Government Accountability Office. *Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight.* Washington DC: U.S. Government Accountability Office, 2012.

U.S. Government Accountability Office. *Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage.* Washington DC: U.S. Government Accountability Office, 2012.

U.S. Government Accountability Office. *Internet Infrastructure: DHS Faces Challenges In Developing a Joint Public/private Recovery Plan.* Report to Congressional Requesters, Washington, D.C: U.S. Government Accountability Office, 2006.

U.S. Govt. Accountability Office. *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use.* Report to Congressional Committees, Washington, D.C.: U.S. Govt. Accountability Office, 2011.

U.S. Govt. Accountability Office. *Critical Infrastructure Protection: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology.* Report to the Congressional Requesters, Washington, D.C.: U.S. Govt. Accountability Office, 2014.

U.S. Govt. Accountability Office. *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented.* Report to Congressional Requestors, Washington, D.C.: U.S. Govt. Accountability Office, 2013.

U.S. Govt. Accountability Office. *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative.* Report to Congressional Requesters, Washinton, D.C.: U.S. Govt. Accountability Office, 2010.

U.S. Govt. Accountability Office. *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed.* Report to Congressional Requesters, Washington, D.C.: U.S. Govt. Accountability Office, 2010.

U.S. Govt. Accountability Office. *Cyberspace: United States Faces Challenges In Addressing Global Cybersecurity and Governance* . Report to Congressional Requesters, Washington, D.C.: U.S. Govt. Accountability Office, 2010.

United States Senate, One Hundred Sixth Congress. *Internet Security: Hearing before the Subcommittee On Communications of the Committee On Commerce, Science, and Transportation.* Second Session, Washington, D.C.: G.P.O., 2000.

US Investigations Services. *USIS Comments on Recent Self-Reported Cyber-Attack on Corporate Network* . August 6, 2014. http://www.usis.com/Media-Release-Detail.aspx?dpid=151 (accessed April 2, 2015).

Verizon. *The 2013 Data Breach Investigations Report.* Verizon, 2013.

Weiss, N. Eric, and Rena S. Miller. *The Target and Other Financial Data Breaches: Frequently Asked Questions.* Report, International Security

& Counter Terrorism Reference Center, Congressional Research Service, Washington, D.C.: Congressional Research Service, 2014, 1-33.

Wortzel, Larry M. *"Cyber Espionage and the Theft of U.S. Intellectual Property and Technology"* . Testimony, House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations , 2013.

Zhang, Zhen. "Cyberwarfare Implications for Critical Infrastructure Sectors." *The Homeland Security Review* 5, no. 3 (Fall 2001): 281-295.

Curriculum Vitae

Alex Leon

Arlington, VA
Alex.D.Leon@gmail.com

EDUCATION

2015* Johns Hopkins University, Master of Arts, Global Security Studies
2012 University of Phoenix, Bachelor of Science, Management
2007 Columbus State Community College, Associate of Arts, Sociology

PROFESSIONAL EXPERIENCE

Senior Strategist with nineteen years of diverse work experience supporting the Department of Defense and other government agencies in both permissive and austere environments. Most recent work focuses on developing enterprise level information operations methods for managing pressing national security challenges exercising a comprehensive understanding of government-wide strategic priorities and the processes required to implement them throughout the DoD.

2012 – Present
Senior Strategist, Modern Technology Solutions Inc.
Office of the Secretary of Defense, Strategic Capabilities Office

* (Expected Summer of 2015)